CAPITULO V

LOS POLINOMIOS Y SUS RAICES

§ 20. Operaciones con los polinomios

La teoría de los determinantes y la teoría de los sistemas de ecuaciones lineales es un desarrollo directo de la rama del álgebra escolar que, comenzando por una ecuaci n de primer grado con una incógnita, nos lleva a los sistemas de dos y tres ecuaciones de primer grado con dos y tres incógnitas, respectivamente. Otra rama del álgebra elemental, considerada más importante, consiste en el *paso de una ecuación de primer grado con una incógnita a una ecuación cuadrática arbitraria, de nuevo con una incógnita, y después a unos tipos particulares de ecuaciones de tercero y cuarto grado.* Esta rama se desarrolla en una amplia y rica sección del álgebra superior dedicada al estudio de ecuaciones arbitrarias de n-ésimo grado con una incógnita. Esta sección del álgebra es la más antigua. El presente capítulo, así como algunos de los capítulos ulteriores del libro están relacionados con esta sección.

La forma general de una ecuación de n-ésimo grado (donde n es *cierto número entero positivo*) es

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0. \tag{1}$$

Se supondrá que los coeficientes a_0, a_1, ..., a_{n-1}, a_n son números complejos arbitrarios y que el *coeficiente superior* a_0 es diferente de cero.

Resolver la ecuación (1) significa hallar para la incógnita x *unos valores numéricos que* satisfagan *a esta ecuación, es decir, que* al sustituirlos en lugar de la incógnita, después de realizar todas las operaciones indicadas, reduzcan a cero el primer miembro de la ecuación (1).

Por otra parte, resulta conveniente sustituir el problema de la resolución de la ecuación (1) por el problema más general del estudio del primer miembro de esta ecuación

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \tag{2}$$

denominado *polinomio de grado n en la indeterminada x.* Hay que tener presente que ahora denominamos polinomio a una expresión de la forma (2), o sea, a una suma de potencias no negativas de la indeterminada x, tomadas con ciertos coeficientes numéricos, y no a cualquier suma de monomios como ocurría en el álgebra elemental. En particular, no se denominarán polinomios las expresiones que contengan la indeterminada x con exponentes negativos o fraccionarios, por ejemplo, $2x^2 - \frac{1}{x} + 3$, o $ax^{-3} + bx^{-2} + cx^{-1} + d + ex + fx^2$, o bien, $x^{\frac{1}{2}} + 1$. Abreviadamente, los polinomios se designarán con las notaciones: $f(x)$, $g(x)$, $\varphi(x)$, etc.

Dos polinomios $f(x)$ y $g(x)$ se supondrán *iguales* (o *idénticamente iguales*), $f(x) = g(x)$, si son idénticos los coeficientes de potencias iguales de la indeterminada. En particular, un polinomio no puede ser idéntico a cero, si al menos uno de sus coeficientes es diferente de cero y, por lo tanto, el signo de igualdad que figura en la expresión de la ecuación de n-ésimo grado (1) no tiene que ver nada con la igualdad de los polinomios que acabamos de definir. El signo $=$ que liga a los polinomios se debe entender como una identidad de los mismos.

Por consiguiente, el polinomio de n-ésimo grado (2) se debe interpretar como una expresión formal, completamente determinada por el conjunto de sus coeficientes $a_0, a_1, \ldots, a_n$, donde $a_0 \neq 0$. El significado exacto de estas palabras se aclarará mucho más tarde, en el cap. 10. Obsérvese que además de la expresión del polinomio en la forma (2), o sea, según las *potencias decrecientes de la indeterminada* x, se permitirán también otras expresiones obtenidas de (2) permutando los sumandos, como por ejemplo, la expresión según las *potencias crecientes de la indeterminada*.

Naturalmente, se podría interpretar el polinomio (2) desde el punto de vista del análisis matemático, o sea, como una función compleja de la variable compleja x. Sin embargo, se debe tener en cuenta que *dos funciones se suponen iguales cuando son iguales sus valores para cualesquiera valores de la variable* x. Está claro que dos polinomios que son iguales en el sentido algebraico formal indicado anteriormente, serán también iguales como funciones de x. Lo recíproco se demostrará en el § 24. Después de esto resultarán equivalentes los puntos de vista algebraico y teórico—funcional sobre el concepto de polinomio con coeficientes numé icos; por ahora tendremos que indicar cada vez el sentido que se da al concepto de polinomio. En el párrafo presente y en los dos que siguen se considerará el polinomio como una expresión algebraica formal.

Por supuesto, para cualquier número natural n existen polinomios de n grado. Examinando todos los polinomios posibles, además de los polinomios de primer grado, cuadráticos, cúbicos y etc., nos encontraremos con *polinomios de grado cero*, es decir, con números complejos **diferentes de cero.** El número cero también se tomará como polinomio; éste es el único polinomio cuyo grado es indefinido.

A continuación definiremos las operaciones de adición y multiplicación para los polinomios de coeficientes complejos. Estas operaciones se introducirán del mismo modo que las operaciones con los polinomios de coeficientes reales, conocidas por el lector en el curso de álgebra elemental.

Dados los polinomios $f(x)$ y $g(x)$ de coeficientes complejos, expresados para mayor comodidad según las potencias crecientes de x:

$$f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n, \qquad a_n \neq 0,$$
$$g(x) = b_0 + b_1x + \ldots + b_{s-1}x^{s-1} + b_sx^s, \qquad b_s \neq 0,$$

donde $n \geqslant s$, se llamará *suma* al polinomio

$$f(x) + g(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1} + c_nx^n,$$

cuyos coeficientes se obtienen sumando los coeficientes respectivos de iguales potencias de la indeterminada en las expresiones de $f(x)$ y $g(x)$, o sea,

$$c_i = a_i + b_i, \quad i = 0, 1, \ldots, n, \tag{3}$$

donde, para $n > s$, se tiene que suponer que los coeficientes b_{s+1}, b_{s+2}, ..., b_n son iguales a cero. El grado de la suma será igual a n, si n es mayor que s; pero, para $n = s$, puede ocurrir que éste sea menor que n, precisamente cuando $b_n = -a_n$.

Se llama *producto* de los polinomios $f(x)$ y $g(x)$ al polinomio

$$f(x) \cdot g(x) = d_0 + d_1x + \ldots + d_{n+s-1}x^{n+s-1} + d_{n+s}x^{n+s},$$

cuyos coeficientes se determinan del modo siguiente:

$$d_i = \sum_{k+l=i} a_kb_l, \quad i = 0, 1, \ldots, n+s-1, \; n+s, \tag{4}$$

o sea, el coeficiente d_i es el resultado de sumar todos los productos de aquellos coeficientes de los polinomios $f(x)$ y $g(x)$ la suma de cuyos índices es igual a i; en particular, $d_0 = a_0b_0$, $d_1 = a_0b_1 + a_1b_0$, ..., $d_{n+s} = a_nb_s$. De la última igualdad resulta la desigualdad $d_{n+s} \neq 0$. Por consiguiente, el *grado del producto de dos polinomios es igual a la suma de sus grados.*

De aquí se deduce que *nunca será igual a cero el producto de polinomios, diferentes de cero.*

Para los polinomios, ¿qué propiedades poseen las operaciones introducidas? Las **propiedades conmutativa y asociativa de la suma** son consecuencia inmediata del cumplimiento de estas propiedades para la suma de los números, puesto que se suman los coeficientes de cada potencia de la indeterminada por separado. La **resta** resulta posible: desempeña el papel del **cero** el número cero, que fue incluido como polinomio; el **opuesto** al polinomio $f(x)$, escrito anteriormente, es el polinomio

$$-f(x) = -a_0 - a_1x - \ldots - a_{n-1}x^{n-1} - a_nx^n.$$

La **propiedad conmutativa de la multiplicación** es consecuencia del cumplimiento de la propiedad conmutativa para el producto de los números y de que en la definición del producto de polinomios, los coeficientes de ambos factores $f(x)$ y $g(x)$ se empleen de un modo equivalente. La propiedad **asociativa** se demuestra del modo siguiente: si, además de los polinomios $f(x)$ y $g(x)$ escritos anteriormente, es dado también el polinomio

$$h(x) = c_0 + c_1x + \ldots + c_{t-1}x^{t-1} + c_tx^t, \quad c_t \neq 0,$$

el coeficiente de x^i, $i = 0, 1, \ldots, n+s+t$ en el producto $[f(x) \times \times g(x)]\,h(x)$ será el número

$$\sum_{j+m=i} \Big(\sum_{k+l=j} a_kb_l \Big) c_m = \sum_{k+l+m=i} a_kb_lc_m,$$

mientras que en el producto $f(x)\,[g(x)\,h(x)]$, será el número

$$\sum_{k+j=i} a_k \Big(\sum_{l+m=j} b_lc_m \Big) = \sum_{k+l+m=i} a_kb_lc_m.$$

que es igual a él.

Finalmente, el cumplimiento de la **ley distributiva** se deduce de la igualdad

$$\sum_{k+l=i} (a_k + b_k)\,c_l = \sum_{k+l=i} a_kc_l + \sum_{k+l=i} b_kc_l,$$

puesto que el primer miembro de ésta es el coeficiente de x^i en el polinomio $[f(x) + g(x)]\,h(x)$ y el segundo miembro es el coeficiente de la misma potencia de la indeterminada en el polinomio $f(x)\,h(x) + g(x)\,h(x)$.

Obsérvese que en el producto de los polinomios, el número 1, considerado como polinomio de grado cero, desempeña el papel de la **unidad.** Por otra parte, el *polinomio $f(x)$ posee un polinomio recíproco $f^{-1}(x)$,*

$$f(x)\,f^{-1}(x) = 1, \tag{5}$$

cuando, y sólo cuando, $f(x)$ es un polinomio de grado cero. En efecto, si $f(x)$ es un número a, diferente de cero, el polinomio recíproco es el número a^{-1}. Pero si $f(x)$ es de grado $n \geqslant 1$, el grado del primer miembro de la igualdad (5), en caso de que existiese el polinomio $f^{-1}(x)$ no sería menor de n, mientras que en el segundo miembro figura un polinomio de grado cero.

De aquí se deduce que *para el producto de polinomios no existe la operación inversa, la división.* En este sentido, el sistema de todos los polinomios de coeficientes complejos se parece al sistema de todos los números enteros. Esta analogía se manifiesta en que para los polinomios, al igual que para los números enteros, subsiste el **algoritmo de la división con resto***. Para el caso de los polinomios de coeficientes reales el lector ya conoce este algoritmo por el álgebra elemental. Pero, como consideramos ahora el caso de polinomios con *coeficientes complejos*, tendremos que hacer todos los enunciados due aquí se requieren y las demostraciones correspondientes.

Para cualesquiera dos polinomios $f(x)$ y $g(x)$ se pueden hallar unos polinomios $q(x)$ y $r(x)$, de tal manera que

$$f(x)=g(x)\,q(x)+r(x), \tag{6}$$

donde el grado de $r(x)$ es menor que el de $g(x)$, o bien, $r(x)=0$. Los polinomios $q(x)$ y $r(x)$ que satisfacen a esta condición se determinan unívocamente.

Demostremos primero la segunda parte del teorema. Supongamos que existen también unos polinomios $\bar{q}(x)$ y $\bar{r}(x)$ que satisfacen a la condición

$$f(x)=g(x)\,\bar{q}(x)+\bar{r}(x), \tag{7}$$

donde el grado de $\bar{r}(x)$ es de nuevo menor que el de $g(x)$**. Igualando entre sí los segundos miembros de las igualdades (6) y (7), se tiene:

$$g(x)\,[q(x)-\bar{q}(x)]=\bar{r}(x)-r(x).$$

El grado del segundo miembro de esta igualdad es menor que el de $g(x)$, mientras que si $q(x)-\bar{q}(x)\neq 0$, el grado del primer miembro sería mayor o igual al grado de $g(x)$. Por esto, tiene que ser $q(x)-\bar{q}(x)=0$, o sea, $q(x)=\bar{q}(x)$, de donde $r(x)=\bar{r}(x)$, como se quería demostrar.

Pasemos a demostrar la primera parte del teorema. Supongamos que n y s son los grados respectivos de los polinomios. Si $n<s$, se puede suponer que $q(x)=0$, $r(x)=f(x)$. Si $n\geqslant s$, aplicaremos el mismo método empleado en álgebra elemental para efectuar la división de polinomios con coeficientes reales, ordenados según las potencias decrecientes de la indeterminada. Sea

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n, \qquad a_0\neq 0,$$
$$g(x)=b_0x^s+b_1x^{s-1}+\ldots+b_{s-1}x+b_s, \qquad b_0\neq 0.$$

Poniendo

$$f(x)-\frac{a_0}{b_0}x^{n-s}g(x)=f_1(x), \tag{8}$$

* Denominada también división entera (*N del T.*).

** O bien $\bar{r}(x)=0$. En adelante, este caso no se va a excluir se obtiene un polinomio cuyo grado es menor que n. Designemos este grado por n_1, y el coeficiente superior del polinomio $f_1(x)$, por a_{10}. Si todavía $n_1 \geqslant s$, ponemos

$$f_1(x) - \frac{a_{10}}{b_0} x^{n_1-s} g(x) = f_2(x), \tag{8_1}$$

designamos con n_2 el grado y con a_{20}, el coeficiente superior del polinomio $f_2(x)$, poniendo después

$$f_2(x) - \frac{a_{20}}{b_0} x^{n_2-s} g(x) = f_3(x), \tag{8_2}$$

y etc.

Como los grados de los polinomios $f_1(x)$, $f_2(x)$, ... decrecen, $n > n_1 > n_2 > \ldots$, después de repetir este proceso un número finito de veces, obtendremos un polinomio $f_k(x)$:

$$f_{k-1}(x) - \frac{a_{k-1,\,0}}{b_0} x^{n_{k-1}-s} g(x) = f_k(x), \tag{8_{k-1}}$$

cuyo grado n_k será menor que s, terminando así el proceso. Sumando ahora las igualdades (8), (8_1), ..., (8_{k-1}), se obtiene:

$$f(x) - \left(\frac{a_0}{b_0} x^{n-s} + \frac{a_{10}}{b_0} x^{n_1-s} + \ldots + \frac{a_{k-1,\,0}}{b_0} x^{n_{k-1}-s}\right) g(x) = f_k(x),$$

o sea, que los polinomios

$$q(x) = \frac{a_0}{b_0} x^{n-s} + \frac{a_{10}}{b_0} x^{n_1-s} + \ldots + \frac{a_{k-1,\,0}}{b_0} x^{n_{k-1}-s},$$
$$r(x) = f_k(x)$$

satisfacen verdaderamente a la igualdad (6), siendo realmente el grado de $r(x)$ menor que el de $g(x)$.

Obsérvese que el polinomio $q(x)$ se llama *cociente* de la división de $f(x)$ por $g(x)$ y $r(x)$, *resto* (o *residuo*) de esta división.

De la consideración del algoritmo de la división con resto, se establece fácilmente que si $f(x)$ y $g(x)$ *son polinomios de coeficientes reales, los coeficientes de todos los polinomios* $f_1(x)$, $f_2(x)$, ..., *y, por consiguiente, también los del cociente* $q(x)$ *y los del resto,* $r(x)$, *son reales.*

§ 21. Divisores. Máximo común divisor

Sean dados unos polinomios $f(x)$ y $\varphi(x)$, diferentes de cero, con coeficientes complejos. Si el resto de la división de $f(x)$ por $\varphi(x)$ es igual a cero, o como también se dice, si $f(x)$ *se divide* (o *es divisible*) por $\varphi(x)$, entonces el polinomio $\varphi(x)$ se llama *divisor* del polinomio $f(x)$.

El polinomio $\varphi(x)$ *es divisor del polinomio* $f(x)$ *si, y sólo si, existe un polinomio* $\psi(x)$ *que satisfaga a la igualdad*

$$f(x)=\varphi(x)\,\psi(x). \tag{1}$$

En efecto, si $\varphi(x)$ es divisor de $f(x)$, el cociente de la división de $f(x)$ por $\varphi(x)$ desempeña el papel de $\psi(x)$. Recíprocamente, supongamos que existe un polinomio $\psi(x)$ que satisface a la igualdad (1). De la unicidad de los polinomios $q(x)$ y $r(x)$ que satisfacen a la igualdad

$$f(x)=\varphi(x)\,q(x)+r(x).$$

demostrada en el párrafo anterior, y de la condición de que el grado de $r(x)$ es menor que el de $\varphi(x)$, se deduce que en este caso el cociente de la división de $f(x)$ por $\varphi(x)$ es igual a $\psi(x)$ y el resto es igual a cero.

Se comprende que, cumpliéndose la igualdad (1), $\psi(x)$ es también divisor de $f(x)$. Luego, es evidente que el grado de $\varphi(x)$ no es superior al de $f(x)$.

Obsérvese que, si el polinomio $f(x)$ y su divisor $\varphi(x)$ tienen ambos coeficientes racionales o reales, el polinomio $\psi(x)$ también tiene los coeficientes racionales o, respectivamente, reales, puesto que éste se halla mediante el algoritmo de la división. Por supuesto, un polinomio de coeficientes racionales o reales puede poseer también divisores cuyos coeficientes no sean todos racionales o, respectivamente, reales. Esto se observa, por ejemplo, en la igualdad

$$x^2+1=(x-i)(x+i).$$

Señalemos algunas propiedades fundamentales de la divisibilidad de los polinomios que tendrán numerosas aplicaciones a continuación.

I. *Si* $f(x)$ *es divisible por* $g(x)$ y $g(x)$ es divisible por $h(x)$, *entonces* $f(x)$ *es divisible por* $h(x)$.

En efecto, por la condición $f(x)=g(x)\,\varphi(x)$ y $g(x)=h(x)\,\psi(x)$, y, por lo tanto, $f(x)=h(x)\,[\psi(x)\,\varphi(x)]$.

II. *Si* $f(x)$ *y* $g(x)$ *es divisible por* $\varphi(x)$, *su suma y diferencia también es divisible por* $\varphi(x)$.

En efecto, de las igualdades $f(x)=\varphi(x)\,\psi(x)$ y $g(x)=\varphi(x)\,\chi(x)$ resulta: $f(x)\pm g(x)=\varphi(x)\,[\psi(x)\pm\chi(x)]$.

III. *Si* $f(x)$ *es divisible por* $\varphi(x)$, *el producto de* $f(x)$ *por cualquier po inomio* $g(x)$ *también es divisible por* $\varphi(x)$.

En efecto, si $f(x)=\varphi(x)\,\psi(x)$, se tiene: $f(x)\,g(x)=\varphi(x)\,[\psi(x)\,g(x)]$.

De II y III se deduce la siguiente propiedad:

IV. *Si cada uno de los polinomios* $f_1(x), f_2(x), \ldots, f_k(x)$ *es divisible por* $\varphi(x)$, *el polinomio*

$$f_1(x)\,g_1(x)+f_2(x)\,g_2(x)+\ldots+f_k(x)\,g_k(x),$$

donde $g_1(x)$, $g_2(x)$, ... $g_k(x)$ *son unos polinomios arbitrarios, también es divisible por* $\varphi(x)$.

V. *Todo polinomio* $f(x)$ *es divisible por cualquier polinomio de grado cero.*

En efecto, si $(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, y c es un número arbitrario, diferente de cero, o sea, un polinomio arbitrario de grado cero, entonces

$$f(x) = c\left(\frac{a_0}{c}x^n + \frac{a_1}{c}x^{n-1} + \ldots + \frac{a_n}{c}\right).$$

VI. *Si* $f(x)$ *es divisible por* $\varphi(x)$, $f(x)$ *es también divisible por* $c\varphi(x)$, *donde* c *es un número arbitrario, diferente de cero.*

En efecto, de la igualdad $f(x) = \varphi(x)\psi(x)$ resulta la igualdad $f(x) = [c\varphi(x)]\cdot[c^{-1}\psi(x)]$.

VII. *Los polinomios* $cf(x)$, $c \neq 0$, *y sólo éstos, son los divisores del polinomio* $f(x)$ *que tienen el mismo grado que* $f(x)$.

En efecto, $f(x) = c^{-1}\{cf(x)\}$, o ea, $f(x)$ es divisible por $cf(x)$.

Si, por otra parte, $f(x)$ es divisible por $\varphi(x)$, coincidiendo los grados de $f(x)$ y $\varphi(x)$, el grado del cociente de la división de $f(x)$ por $\varphi(x)$ tiene que ser igual a cero, es decir, $f(x) = d\varphi(x)$, $d \neq 0$, de donde $\varphi(x) = d^{-1}f(x)$.

De aquí resulta la siguiente propiedad:

VIII. *Los polinomios* $f(x)$ *y* $g(x)$ *son divisibles entre sí cuando, y sólo cuando,* $g(x) = cf(x)$, $c \neq 0$.

Finalmente, de VIII y I resulta la propiedad:

IX. *Todo divisor de uno de los dos polinomios* $f(x)$ y $cf(x)$, donde $c \neq 0$, es divisor del otro.

Máximo común divisor. Sean dados unos polinomios arbitrarios, $f(x)$ y $g(x)$. El polinomio $\varphi(x)$ se llama *divisor común* de $f(x)$ y $g(x)$, si es divisor de cada uno de estos polinomios. La propiedad *V* (véase más arriba) muestra que todos los polinomios de grado cero pertenecen al conjunto de los divisores comunes de los polinomios $f(x)$ y $g(x)$. Si éstos no tienen más divisores comunes, se dice que *son primos entre sí*.

En el caso general, los polinomios $f(x)$ y $g(x)$ pueden poseer divisores dependientes de x. Introduzcamos ahora el concepto de *máximo* común divisor de estos polinomios.

Sería incómodo tomar tal definición, según la cual el máximo común divisor de los polinomios sería el común divisor de mayor grado. Por una parte, no sabemos todavía si $f(x)$ y $g(x)$ pueden poseer o no muchos divisores comunes distintos de mayor grado, que no sólo se diferencien entre sí en un factor de grado cero, por lo que esta definición resultaría muy indeterminada. Por otra parte, el lector ya conocerá por la aritmética elemental la forma de obtener el máximo común divisor de números enteros, y sabrá que el máximo común divisor 6 de los números enteros 12 y 18, no sólo es el mayor de los divisores comunes de estos números, sino que también es divisible por cualquier otro de sus divisores comunes; en efecto, los demás divisores comunes de los números 12 y 18 son: 1, 2, 3, -1, -2, -3, -6.

Por consiguiente, para el caso de los polinomios, aceptaremos la siguiente definición:

Se llama *máximo común divisor* de los polinomios $f(x)$ y $g(x)$, diferentes de cero, al polinomio $d(x)$ que es común divisor y que a la vez es divisible por cualquier otro divisor común de estos polinomios. El *máximo común divisor* de los polinomios $f(x)$ y $g(x)$ se designa con la notación $(f(x), g(x))$.

Con esta definición no se aclara el problema de la existencia del máximo común divisor para cualesquiera polinomios $f(x)$ y $g(x)$. Ahora se dará una respuesta positiva a este problema. A la vez, se señalará un método para hallar el máximo común divisor de los polinomios dados. Por supuesto, aquí no se puede emplear el método con el que ordinariamente se halla el máximo común divisor de los números enteros, puesto que para los polinomios no tenemos por ahora nada parecido a la descomposición del número entero en un producto de factores primos. Sin embargo, para los números enteros existe también otro método, denominado *algoritmo de las divisiones sucesivas* o *algoritmo de Euclides*; este método también puede aplicarse a los polinomios.

El algoritmo de Euclides para los polinomios consiste en lo siguiente. Sean dados los polinomios $f(x)$ y $g(x)$. Se divide $f(x)$ por $g(x)$ y se obtiene por lo general un resto $r_1(x)$. Se divide luego $g(x)$ por $r_1(x)$ y se obtiene el resto $r_2(x)$, se divide $r_1(x)$ por $r_2(x)$, etc. Como los grados de los restos van disminuyendo todo el tiempo, en esta cadena de divisiones sucesivas llegaremos a un lugar en el que la división será exacta y el proceso se terminará. *El resto $r_k(x)$, por el que se divide exactamente el resto anterior $r_{k-1}(x)$, será el máximo común divisor de los polinomios $f(x)$ y $g(x)$.*

Para la demostración, escribamos lo expuesto en las líneas anteriores en forma de la siguiente cadena de igualdades:

$$\left.\begin{aligned} f(x) &= g(x)\,q_1(x) + r_1(x), \\ g(x) &= r_1(x)\,q_2(x) + r_2(x), \\ r_1(x) &= r_2(x)\,q_3(x) + r_3(x), \\ &\cdots\cdots\cdots\cdots\cdots \\ r_{k-3}(x) &= r_{k-2}(x)\,q_{k-1}(x) + r_{k-1}(x), \\ r_{k-2}(x) &= r_{k-1}(x)\,q_k(x) + r_k(x), \\ r_{k-1}(x) &= r_k(x)\,q_{k+1}(x). \end{aligned}\right\} \qquad (2)$$

La última igualdad muestra que $r_k(x)$ es divisor de $r_{k-1}(x)$. De aquí resulta que ambos sumandos del segundo miembro de la penúltima igualdad son divisibles por $r_k(x)$, y por lo tanto, $r_k(x)$ también es divisor de $r_{k-2}(x)$. A continuación, subiendo del mismo modo a los otros renglones, obtenemos que $r_k(x)$ también es divisor de $r_{k-3}(x), \ldots, r_2(x), r_1(x)$. De aquí, en virtud de la segunda igualdad, resulta que $r_k(x)$ es divisor de $g(x)$, de donde, en virtud de la primera igualdad, también es divisor de $f(x)$. Por lo tanto, $r_k(x)$ es un divisor común de $f(x)$ y $g(x)$.

Consideremos ahora un divisor común arbitrario $\varphi(x)$ de los polinomios $f(x)$ y $g(x)$. Como el primer miembro y el primer sumando del segundo miembro de la primera de las igualdades (2) son divisibles por $\varphi(x)$, $r_1(x)$ también es divisible por $\varphi(x)$. Pasando a la segunda y a las siguientes igualdades, obtenemos del mismo modo que todos los polinomios $r_2(x), r_3(x), \ldots$, son divisibles por $\varphi(x)$. Si, finalmente, se ha demostrado que $r_{k-2}(x)$ y $r_{k-1}(x)$ son divisibles por $\varphi(x)$, de la penúltima igualdad obtenemos que $r_k(x)$ es divisible por $\varphi(x)$. Por lo tanto, $r_k(x)$ es verdaderamente el máximo común divisor de $f(x)$ y $g(x)$.

Por consiguiente, hemos demostrado que dos polinomios cualesquiera poseen máximo común divisor y hemos obtenido un método para su cálculo. Este método muestra que, *si los polinomios $f(x)$ y $g(x)$ tienen ambos coeficientes racionales o reales, los coeficientes de su máximo común divis r también son racionales o, respectivamente, reales*, a pesar de que estos polinomios pueden tener divisores cuyos coeficientes no sean todos racionales (reales). Así, pues, los polinomios con coeficientes racionales

$$f(x) = x^3 - 3x^2 - 2x + 6, \quad g(x) = x^3 + x^2 - 2x - 2$$

tienen un máximo común divisor $x^2 - 2$ con coeficientes racionales, a pesar de que tienen un común divisor $x - \sqrt{2}$ cuyos coeficientes no son todos racionales.

Si $d(x)$ es el máximo común divisor de los polinomios $f(x)$ y $g(x)$, como muestran las propiedades VIII y IX (véase la pág. 139), por máximo común divisor se podría tomar también el polinomio $cd(x)$, donde c es un número arbitrario, diferente de cero. En otras palabras, el *máximo común divisor de dos polinomios se determina salvo un factor de grado cero*. En virtud de esto, se puede convenir en que el **coeficiente superior del máximo común divisor de dos polinomios sea siempre igual a la unidad.** Aplicando esta condición, se puede afirmar que *dos polinomios son primos entre sí cuando, y sólo cuando, su máximo común divisor es igual a la unidad*. En efecto, por máximo común divisor de dos polinomios, primos entre sí, se puede tomar cualquier número diferente de cero; pero si este número se multiplica por su elemento recíproco, obtenemos la unidad.

Ejemplo. Hallar el máximo común divisor de los polinomios

$$f(x)=x^4+3x^3-x^2-4x-3,\quad g(x)=3x^3+10x^2+2x-3.$$

Para evitar coeficientes fraccionarios, al aplicar el algoritmo de Euclides a los polinomios con coeficientes enteros, se puede multiplicar el dividendo o simplificar el divisor por cualquier número diferente de cero, no sólo al comenzar alguna de las divisiones sucesivas, sino también durante el proceso de la división misma. Naturalmente, esto conducirá a una alteración del cociente, pero los restos que nos interesan adquirirán solamente un factor de grado cero, lo que, como ya sabemos, al buscar el máximo común divisor, es admisible.

Dividimos $f(x)$ por $g(x)$, multiplicando previamente $f(x)$ por 3:

$$\begin{array}{r|l} 3x^4+9x^3-3x^2-12x-9 & 3x^3+10x^2+2x-3 \\ \cline{2-2} \underline{3x^4+10x^3+2x^2-3x} & x+1 \\ -x^3-5x^2-9x-9 & \end{array}$$

(multiplicamos por -3)

$$\begin{array}{r} 3x^3+15x^2+27x+27 \\ \underline{3x^3+10x^2+2x-3} \\ 5x^2+25x+30. \end{array}$$

Por lo tanto, después de simplificar por 5, el primer resto es $r_1(x)=$ $=x^2+5x+6$. Dividimos el polinomio $g(x)$ por éste:

$$\begin{array}{r|l} 3x^3+10x^2+2x-3 & x^2+5x+6 \\ \cline{2-2} \underline{3x^3+15x^2+18x} & 3x-5 \\ -5x^2-16x-3 & \\ \underline{-5x^2-25x-30} & \\ 9x+27. & \end{array}$$

Por consiguiente, después de simplificar por 9, el segundo resto es: $r_2(x)=x+3$. Como

$$r_1(x)=r_2(x)(x+2),$$

$r_2(x)$ será el último resto, por el que se divide exactamente el resto anterior. Por lo tanto, éste es el máximo común divisor:

$$(f(x),\ g(x))=x+3.$$

Apliquemos el algoritmo de Euclides para la demostración del **teorema** siguiente:

Si $d(x)$ *es el máximo común divisor de los polinomios* $f(x)$ *y* $g(x)$, *existen tales polinomios* $u(x)$ *y* $v(x)$ *que*

$$f(x)\,u(x)+g(x)\,v(x)=d(x). \tag{3}$$

Siempre se puede suponer que, si los grados de los polinomios $f(x)$ *y* $g(x)$ *son mayores que cero, el grado de* $u(x)$ *es menor que el grado de* $g(x)$ *y el grado de* $v(x)$ *es menor que el grado de* $f(x)$.

La demostración está basada en las igualdades (2). Si se tiene en cuenta que $r_k(x)=d(x)$ y se pone $u_1(x)=1$, $v_1(x)=-q_k(x)$, según la penúltima de las igualdades (2), se tiene:

$$d(x)=r_{k-2}(x)\,u_1(x)+r_{k-1}(x)\,v_1(x).$$

Poniendo aquí la expresión de $r_{k-1}(x)$ mediante $r_{k-3}(x)$ y $r_{k-2}(x)$, se obtiene de la igualdad anterior (2):

$$d(x) = r_{k-3}(x)\, u_2(x) + r_{k-2}(x)\, v_2(x),$$

donde, evidentemente, $u_2(x) = v_1(x)$, $v_2(x) = u_1(x) - v_1(x)\, q_{k-1}(x)$. Continuando el ascenso por las igualdades (2), se llegará, finalmente, a la igualdad (3) que se quería demostrar.

Para la demostración de la segunda afirmación del teorema, supongamos que se han hallado ya los polinomios $u(x)$ y $v(x)$ que satisfacen a la gualdad (3), pero que el grado de $u(x)$ es, por ejemplo, mayor o igual al grado de $g(x)$. Dividamos $u(x)$ por $g(x)$:

$$u(x) = g(x)\, q(x) + r(x),$$

donde el grado de $r(x)$ es menor que el grado de $g(x)$, e introduzcamos esta expresión en (3). Se obtiene la igualdad.

$$f(x)\, r(x) + g(x)\, [v(x) + f(x)]q(x)] = d(x).$$

El grado del factor que figura con $f(x)$ es ya menor que el grado de $g(x)$. Por otra parte, el grado del polinomio que figura entre corchetes es menor que el grado de $f(x)$, puesto que, en caso contrario, el grado del segundo sumando del primer miembro no sería menor que el grado del producto $g(x)\, f(x)$, y como el grado del primer sumando es menor que el grado de este producto, todo el primer miembro sería de grado mayor o igual a $g(x)\, f(x)$, mientras que según nuestra suposición, el polinomio $d(x)$ es de menor grado.

Así el teorema queda demostrado. A la vez, tenemos que, si los polinomios $f(x)$ y $g(x)$ tienen coeficientes racionales o reales, los polinomios $u(x)$ y $v(x)$ que satisfacen a la igualdad (3) se pueden elegir de modo que sus coeficientes sean racionales o, respectivamente, reales.

Ejemplo. Hallemos los polinomios $u(x)$ y $v(x)$ que satisfacen a la igualdad (3), si

$$f(x) = x^3 - x^2 + 3x - 10, \quad g(x) = x^3 + 6x^2 - 9x - 14.$$

Apliquemos el algoritmo de Euclides a estos polinomios: ahora, al efectuar las divisiones ya no se puede permitir ninguna alteración de los cocientes, puesto que éstos se emplean para hallar los polinomios $u(x)$ y $v(x)$. Obtenemos el siguiente sistema de igualdades:

$$f(x) = g(x) + (-7x^2 + 12x + 4);$$

$$g(x) = (-7x^2 + 12x + 4)\left(-\frac{1}{7}x - \frac{54}{49}\right) + \frac{235}{49}(x-2);$$

$$-7x^2 + 12x + 4 = (x-2)(-7x-2).$$

De aquí sale que $(f(x), g(x)) = x - 2$ y que

$$u(x) = \frac{7}{235}x + \frac{54}{235}, \quad v(x) = -\frac{7}{235}x - \frac{5}{235}.$$

Aplicando ahora el teorema demostrado a polinomios, primos entre sí, obtenemos el siguiente resultado:

Los polinomios $f(x)$ y $g(x)$ *son primos entre sí cuando, y sólo cuando, existen unos polinomios* $u(x)$ y $v(x)$ *que satisfacen a la igualdad*

$$f(x)\,u(x)+g(x)\,v(x)=1. \tag{4}$$

Basándose en este resultado se pueden demostrar unos cuantos **teoremas sobre los polinomios primos entre sí**, que, aunque sencillos, son importantes:

a) *Si el polinomio* $f(x)$ *es primo con cada uno de los polinomios* $\varphi(x)$ y $\psi(x)$, *también es primo con su producto.*

En efecto, según (4), existen unos polinomios $u(x)$ y $v(x)$ tales que

$$f(x)\,u(x)+\varphi(x)\,v(x)=1.$$

Multiplicando esta igualdad por $\psi(x)$, obtenemos:

$$f(x)\,[u(x)\,\psi(x)]+[\varphi(x)\,\psi(x)]\,v(x)=\psi(x),$$

de donde se deduce que todo común divisor de $f(x)$ y $\varphi(x)\,\psi(x)$ es también divisor de $\psi(x)$; sin embargo, según la condición, $(f(x), \psi(x))=1$.

b) *Si el producto de los polinomios* $f(x)$ *y* $g(x)$ *es divisible por* $\varphi(x)$, *pero* $f(x)$ *y* $\varphi(x)$ *son primos entre sí*, $g(x)$ *es divisible por* $\varphi(x)$.

En efecto, multiplicando la igualdad

$$f(x)\,u(x)+\varphi(x)\,v(x)=1$$

por $g(x)$, obtenemos:

$$[f(x)\,g(x)]\,u(x)+\varphi(x)\,[v(x)\,g(x)]=g(x).$$

Ambos sumandos del primer miembro de esta igualdad son divisibles por $\varphi(x)$; por consiguiente, también $g(x)$ es divisible por $\varphi(x)$.

c) *Si el polinomio* $f(x)$ *es divisible por cada uno de los polinomios* $\varphi(x)$ *y* $\psi(x)$, *que son primos entre sí, entonces* $f(x)$ *también es divisible por su producto.*

En efecto, $f(x)=\varphi(x)\,\overline{\varphi}(x)$, o sea, el producto que figura en el segundo miembro es divisible por $\psi(x)$. Por esto, según b), $\overline{\varphi}(x)$ es divisible por $\psi(x)$, $\overline{\varphi}(x)=\psi(x)\,\overline{\psi}(x)$, de donde $f(x)= =[\varphi(x)\,\psi(x)]\,\overline{\psi}(x)$.

La definición de máximo común divisor se puede generalizar al caso de cualquier sistema finito de polinomios. Se llama *máximo común divisor* de los polinomios $f_1(x), f_2(x), \ldots, f_s(x)$ a su divisor común que es divisible por cualquier otro divisor común de los mismos. La existencia del máximo común divisor para cualquier sistema finito de polinomios es consecuencia del siguiente **teorema**, que facilita también un procedimiento para su cálculo.

El máximo común divisor de los polinomios $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ *es igual al máximo común divisor del polinomio* $f_s(x)$ *y del máximo común divisor de los polinomios* $f_1(x)$, $f_2(x)$, ..., $f_{s-1}(x)$.

En efecto, el teorema es evidente para $s = 2$. Por esto, supondremos que el teorema subsiste para el caso $s - 1$, o sea, que, en particular, ya está demostrada la existencia del máximo común divisor $d(x)$ de los polinomios $f_1(x)$, $f_2(x)$, ..., $f_{s-1}(x)$. Designemos mediante $\overline{d}(x)$ el máximo común divisor de los polinomios $d(x)$ y $f_s(x)$. Es evidente que éste es un divisor común de todos los polinomios dados. Por otra parte, cualquier otro divisor común de estos polinomios es también divisor de $d(x)$ y, por lo tanto, de $\overline{d}(x)$.

En particular, se dice que $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ es un sistema de polinomios, *primos entre sí*, si los únicos divisores comunes de ellos son los polinomios de grado cero, o sea, si su máximo común divisor es igual a 1. Si $s > 2$, puede ocurrir que estos polinomios no sean primos entre sí dos a dos. Así, pues, los polinomios

$$f(x) = x^3 - 7x^2 + 7x + 15,\quad g(x) = x^2 - x - 20,$$
$$h(x) = x^3 + x^2 - 12x$$

son primos entre sí, a pesar de que

$$(f(x),\ g(x)) = x - 5,\quad (f(x),\ h(x)) = x - 3,\quad (g(x),\ h(x)) = x + 4.$$

El lector obtendrá fácilmente la generalización de los teoremas a) — c), demostrados anteriormente, sobre los polinomios primos entre sí, para el caso de cualquier número finito de polinomios

§ 22. Las raíces de los polinomios

En el § 20 nos encontramos con los valores de un polinomio, cuando se hablaba del punto de vista teórico-funcional del concepto de polinomio. Recordemos la definición.

Si

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n, \tag{1}$$

es un polinomio y c es un número, el número

$$f(c) = a_0c^n + a_1c^{n-1} + \ldots + a_n,$$

obtenido por la sustitución de la indeterminada x por el número c, en la expresión (1) de $f(x)$, y por la realización consiguiente de las operaciones indicadas, se denomina *valor del polinomio* $f(x)$ *para* $x = c$. Se comprende que, si $f(x) = g(x)$, en el sentido de la igualdad algebraica de polinomios definida en el § 20, entonces $f(c) = g(c)$ para cualquier c.

Fácilmente se ve también que si

$$\varphi(x) = f(x) + g(x), \quad \psi(x) = f(x)\, g(x),$$

se tiene

$$\varphi(c) = f(c) + g(c), \quad \psi(c) = f(c)\, g(c).$$

En otras palabras, considerando a los polinomios desde el punto de vista teórico-funcional, la suma y el producto de los polinomios definidas en el § 20, se convierten en la suma y el producto de funciones, consideradas en el sentido de la suma y producto de los valores respectivos de estas funciones.

Si $f(c) = 0$, o sea, si el polinomio $f(x)$ se anula al *sustituir el número c en lugar de la indeterminada, c se llama raíz* del polinomio $f(x)$* (o de la ecuación $f(x) = 0$). Ahora se demostrará que este concepto está relacionado con la teoría de la divisibilidad de los polinomios, estudiada en el párrafo anterior.

Si se divide el polinomio $f(x)$ por un polinomio arbitrario de primer grado (o como se dirá a continuación, por un *polinomio lineal*), el resto será un polinomio de grado cero o bien será igual a cero, es decir, siempre será un número r. Aplicando el **teorema** que sigue es fácil hallar este resto sin realizar la división (se supone que el polinomio lineal es de la forma $x - c$).

El resto de la división de un polinomio $f(x)$ por un polinomio lineal $x - c$ es igual al valor $f(c)$ que toma el polinomio $f(x)$ para $x = c$.

En efecto, sea

$$f(x) = (x - c)\, q(x) + r.$$

Tomando los valores de ambos miembros de esta igualdad para $x = c$, obtenemos:

$$f(c) = (c - c)\, q(c) + r = r,$$

lo cual demuestra el teorema.

De aquí se deduce la importante **conclusión**:

El número c es raíz del polinomio $f(x)$ cuando, y sólo cuando, $f(x)$ es divisible por $x - c$.

Por otra parte, es evidente que si $f(x)$ es divisible por algún polinomio de primer grado $ax + b$, es divisible también por el polinomio $x - \left(-\frac{b}{a}\right)$, o sea, por un polinomio de la forma $x - c$. De este modo, la *averiguación de las raíces del polinomio $f(x)$ es equivalente a la averiguación de sus divisores lineales.*

En virtud de lo expuesto anteriormente, el siguiente método de división de un polinomio $f(x)$ por el binomio lineal $x - c$ es de especial interés, pues es más simple que el algoritmo general de di-

* También se dice que c es un cero del polinomio $f(x)$. (*Nota del T.*)

visión de los polinomios. Este método se denomina **regla de Horner.** Sea

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n \tag{2}$$

y supongamos que

$$f(x) = (x-c)\,q(x) + r, \tag{3}$$

donde

$$q(x) = b_0x^{n-1} + b_1x^{n-2} + b_2x^{n-3} + \ldots + b_{n-1}.$$

Igualando en (3) los coeficientes de potencias iguales de x, obtenemos:

$$\begin{aligned} a_0 &= b_0, \\ a_1 &= b_1 - cb_0, \\ a_2 &= b_2 - cb_1, \\ &\ldots\ldots\ldots\ldots \\ a_{n-1} &= b_{n-1} - cb_{n-2}, \\ a_n &= r - cb_{n-1}. \end{aligned}$$

De aquí se deduce que $b_0 = a_0$, $b_k = cb_{k-1} + a_k$, $k = 1, 2, \ldots, n-1$, o sea, se obtiene **el coeficiente** b_k **multiplicando el coeficiente anterior** b_{k-1} **por** c **y agregándole el coeficiente correspondiente** a_k; finalmente, $r = cb_{n-1} + a_n$, es decir, el resto r, que como ya sabemos es igual a $f(c)$, se obtiene por la misma regla. Por lo tanto, los coeficientes del cociente y el resto se pueden obtener sucesivamente mediante unos cálculos del mismo tipo; éstos se realizan de acuerdo a un esquema, como se muestra en los siguientes ejemplos:

1. Dividir $f(x) = 2x^5 - x^4 - 3x^3 + x - 3$ por $x - 3$.

Formemos una tabla colocando sobre la raya los coeficientes del polinomio $f(x)$; bajo la raya se colocan los coeficientes correspondientes del cociente y del resto que se calculan sucesivamente y, a la izquierda, a un lado, el valor dado de c:

$$3\left|\begin{array}{cccccc} 2 & -1 & -3 & 0 & 1 & -3 \\ \hline 2, & 3\cdot 2-1=5, & 3\cdot 5-3=12, & 3\cdot 12+0=36, & 3\cdot 36+1=109, & 3\cdot 109-3=324 \end{array}\right..$$

Por lo tanto, el coeficiente buscado es

$$q(x) = 2x^4 + 5x^3 + 12x^2 + 36x + 109,$$

y el resto, $r = f(3) = 324$.

2. Dividir $f(x) = x^4 - 8x^3 + x^2 + 4x - 9$ por $x + 1$.

$$-1\left|\begin{array}{ccccc} 1 & -8 & 1 & 4 & -9 \\ \hline 1 & -9 & 10 & -6 & -3. \end{array}\right.$$

Por consiguiente, el cociente es

$$q(x) = x^3 - 9x^2 + 10x - 6,$$

y el resto $(r = f(-1)) = -3$

Estos ejemplos muestran que la *regla de Horner se puede utilizar también para calcular rápidamente el valor del polinomio para un valor dado de la indeterminada.*

Raíces múltiples. Si c es una raíz del polinomio $f(x)$, o sea, si $f(c) = 0$, entonces, como ya sabemos $f(x)$ es divisible por $x - c$. Puede ocurrir que $f(x)$ no sólo sea divisible por la primera potencia del binomio lineal $x - c$, sino también por potencias superiores. De todos modos, siempre existirá un número natural k tal que $f(x)$ sea divisible por $(x - c)^k$, pero no por $(x - c)^{k+1}$. En consecuencia,

$$f(x) = (x - c)^k \varphi(x),$$

en donde el polinomio $\varphi(x)$ ya no es divisible por $x - c$, o sea, el número c no es raíz de $\varphi(x)$. El número k se llama orden de *multiplicidad* de la raíz c del polinomio $f(x)$ y el número c, *raíz múltiple* de este polinomio de orden k. Si $k = 1$, se dice que c es una raíz *simple*.

El concepto de raíz múltiple está estrechamente ligado con el concepto de derivada del polinomio. Como estamos estudiando los polinomios con coeficientes complejos cualesquiera, no podemos utilizar directamente el concepto de derivada que se introdujo en el curso de análisis matemático. Todo lo que se diga a continuación se debe considerar como una **definición** de la derivada de un polinomio, independiente del curso de análisis.

Sea dado un polinomio de n-ésimo grado

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

con cualesquiera coeficientes complejos. El polinomio de $(n-1)$-ésimo grado,

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \dots + 2a_{n-2}x + a_{n-1},$$

se llama *derivada* (o *derivada primera*) del polinomio $f(x)$. La derivada de cero y de un polinomio de grado cero se supone igual a cero. La derivada de la derivada primera se llama *derivada segunda* del polinomio $f(x)$ y se designa con $f''(x)$, etc. Es evidente que

$$f^{(n)}(x) = n!\, a_0,$$

por lo cual $f^{(n+1)}(x) = 0$, es decir, la *$(n + 1)$-ésima derivada de un polinomio de n-ésimo grado es igual a cero.*

En el caso de polinomios de coeficientes complejos no podemos utilizar las propiedades de la derivada que fueron demostradas en el curso de análisis para los polinomios de coeficientes reales, sino que tenemos que demostrar de nuevo estas propiedades utilizando solamente la definición de derivada dada anteriormente. Aquí nos interesan las siguientes propiedades que, como se suele decir, representan las fórmulas del derivación de la suma y del producto:

$$(f(x)+g(x))' = f'(x)+g'(x), \tag{4}$$

$$(f(x)\cdot g(x))' = f(x)g'(x)+f'(x)g(x). \tag{5}$$

Estas fórmulas se comprueban fácilmente mediante un cálculo directo, tomando por $f(x)$ y $g(x)$ dos polinomios arbitrarios y aplicando la definición de derivada dada anteriormente; recomendamos al lector hacerlo.

La fórmula (5) se generaliza sin dificultad al caso de un producto de cualquier número finito de factores, de donde, de un modo ordinario, se puede deducir la fórmula para la derivada de una potencia:

$$(f^k(x))' = kf^{k-1}(x)f'(x). \tag{6}$$

Nuestro propósito es demostrar el teorema siguiente:

Si el número c es una raíz k-múltiple del polinomio $f(x)$, entonces, para $k>1$, éste será una raíz $(k-1)$-múltiple de la derivada primera de este polinomio; si $k=1$, el número c no será raíz de $f'(x)$.

En efecto, sea

$$f(x) = (x-c)^k\varphi(x), \quad k\geqslant 1, \tag{7}$$

donde $\varphi(x)$ ya no es divisible por $x-c$. Derivando la igualdad (7), se obtiene:

$$f'(x) = (x-c)^k\varphi'(x)+k(x-c)^{k-1}\varphi(x) =$$
$$= (x-c)^{k-1}[(x-c)\varphi'(x)+k\varphi(x)].$$

El primer término de la suma que figura entre los corchetes es divisible por $x-c$, mientras que el segundo no es divisible por éste; por consiguiente, toda esta suma no puede ser divisible por $x-c$. Teniendo en cuenta que el cociente de la división de $f(x)$ por $(x-c)^{k-1}$ se determina unívocamente, resulta que $(x-c)^{k-1}$ es la máxima potencia del binomio $x-c$ por la cual es divisible el polinomio $f'(x)$, como se quería demostrar.

Aplicando unas cuantas veces este teorema, obtenemos que la *raíz k-múltiple del polinomio $f(x)$ es raíz $(k-s)$-múltiple de la s-ésima derivada de este polinomio $(k\geqslant s)$ y que por primera vez no será raíz para la k-ésima derivada de $f(x)$.*

§ 23. Teorema fundamental

Al estudiar en el párrafo anterior las raíces de los polinomios, no planteamos el problema de la existencia de raíces para cualquier polinomio. Se sabe que existen polinomios de coeficientes reales que no tienen raíces reales como, por ejemplo: x^2+1. Se podría esperar que existiesen polinomios que no tuviesen raíces incluso entre los números complejos, sobre todo si se consideran polinomios con cualesquiera coeficientes complejos. Si esto fuese así, se necesitaría una ampliación ulterior del sistema de los números complejos. Sin embargo, en realidad, subsiste el siguiente **teorema fundamental del álgebra de los números complejos:**

Todo polinomio de cualesquiera coeficientes numéricos, cuyo grado no sea menor que la unidad, tiene por lo menos una raíz, generalmente, compleja.

Este teorema es uno de los adelantos más grandiosos de toda la matemática y encuentra aplicación en las más diversas ramas de la ciencia. En particular, en él se basa toda la teoría ulterior de los polinomios con coeficientes numéricos. Por esta razón, le llamaban antes (y a veces ahora también le llaman) «teorema fundamental del álgebra superior». No obstante, el teorema fundamental no es puramente algebraico. Todas sus demostraciones (después de Gauss, que fue el primero en demostrar este teorema a fines del siglo XVIII, se hallaron muchas otras demostraciones), en tal o cual grado, emplean las llamadas propiedades topológicas de los números reales y complejos, o sea, las propiedades que están ligadas a la continuidad.

En la demostración que se va a exponer ahora, el polinomio $f(x)$ de coeficientes complejos se va a considerar como una función de la variable compleja x. Por lo tanto, x puede tomar cualesquiera valores complejos, o como suele decirse, teniendo en cuenta el método de construcción de los números complejos expuesto en el § 17, la variable x varía en el *plano complejo*. Los valores de la función $f(x)$ también serán números complejos. Se puede suponer que estos valores se señalan en otro ejemplar de plano complejo, del mismo modo que en el caso de las funciones reales de la variable real los valores de la variable independiente se señalan en una recta numérica (eje de abscisas), y los valores de la función, en otra (eje de ordenadas).

La definición de función continua que conoce el lector por el curso de análisis matemático, se generaliza también para la función de la variable compleja, donde en el enunciado de la definición se deben sustituir los valores absolutos por los módulos.

Precisando, la función compleja $f(x)$ de la variable compleja x se llama *continua en el punto* x_0, si para cualquier número real positivo ε se puede elegir un número real positivo δ tal que se cumpla la desigualdad

$$|f(x_0+h)-f(x_0)|<\varepsilon$$

para cualquier incremento h (por lo general, complejo) cuyo módulo satisfaga a la desigualdad $|h|<\delta$. La función $f(x)$ se llama *continua*, si es continua en todos los puntos x_0 en que está definida la función.

Un polinomio $f(x)$ representa una función continua de la variable compleja x.

Se podría efectuar la demostración de este teorema del mismo modo que se hace en el curso de análisis matemático, o sea, demostrando que la suma y el producto de funciones continuas también son continuas y observando que una función que constantemente es igual a un mismo número complejo, es continua. Sin embargo, aquí procederemos de otro modo.

Demostraremos primero un caso particular del teorema: la continuidad de $f(x)$ en el punto $x_0 = 0$, suponiendo que el término independiente del polinomio $f(x)$ es igual a cero. En otras palabras, demostraremos el siguiente lema (en lugar de h se escribirá x):

Lema 1. *Si el término independiente del polinomio $f(x)$ es igual a cero:*

$$f(x) = a_0x^n a_1x^{n-1} + \ldots + a_{n-1}x,$$

o sea, $f(0) = 0$, entonces para cualquier $\varepsilon > 0$ existe un número $\delta > 0$ tal, que $|f(x)| < \varepsilon$ para todos los x que satisfacen a la condición $|x| < \delta$.

En efecto, sea

$$A = \text{máx}\,(|a_0|, |a_1|, \ldots, |a_{n-1}|).$$

Sea dado el número ε. Demostremos que el número

$$\delta = \frac{\varepsilon}{A+\varepsilon}, \tag{1}$$

satisface a las condiciones que se piden.

En efecto,

$$|f(x)| \leqslant |a_0|\,|x|^n + |a_1|\,|x|^{n-1} + \ldots + |a_{n-1}|\,|x| \leqslant$$
$$\leqslant A(|x|^n + |x|^{n-1} + \ldots + |x|),$$

o sea,

$$|f(x)| \leqslant A\frac{|x| - |x|^{n+1}}{1-|x|}.$$

Como $|x| < \delta$ y como, en virtud de (1), $\delta < 1$, se tiene:

$$\frac{|x| - |x|^{n+1}}{1-|x|} < \frac{|x|}{1-|x|},$$

por lo cual,

$$|f(x)| < \frac{A|x|}{1-|x|} < \frac{A\delta}{1-\delta} = \frac{A\dfrac{\varepsilon}{A+\varepsilon}}{1-\dfrac{\varepsilon}{A+\varepsilon}} = \varepsilon,$$

como se quería demostrar.

Deduzcamos ahora la fórmula que sigue. Sea dado un polinomio

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

con cualesquiera coeficientes complejos. Sustituyamos x por la suma $x+h$, donde h es otra indeterminada. Desarrollando en el primer miembro cada una de las potencias $(x+h)^k$, $k\leqslant n$, según la fórmula del binomio, y reuniendo todos los términos con iguales potencias de h, se obtiene la igualdad

$$f(x+h)=f(x)+hf'(x)+\frac{h^2}{2!}f''(x)+\ldots+\frac{h^n}{n!}f^{(n)}(x),$$

que el lector fácilmente puede comprobar, o sea, la *fórmula de Taylor*, que proporciona el desarrollo de $f(x+h)$ en potencias del «incremento» h.

La continuidad de un polinomio arbitrario $f(x)$ en cualquier punto x_0 se demuestra ahora del modo siguiente. En virtud de la fórmula de Taylor,

$$f(x_0+h)-f(x_0)=c_1h+c_2h^2+\ldots+c_nh^n=\varphi(h),$$

donde

$$c_1=f'(x_0),\ c_2=\frac{1}{2!}f''(x_0),\ \ldots,\ c_n=\frac{1}{n!}f^{(n)}(x_0).$$

El polinomio $\varphi(h)$ en la indeterminada h es un polinomio sin término independiente y, por esto, en virtud del lema 1, para cualquier $\varepsilon>0$ existe un $\delta>0$ tal que $|\varphi(h)|<\varepsilon$, o sea,

$$|f(x_0+h)-f(x_0)|<\varepsilon,$$

para $h<\delta$, que es lo que se quería demostrar.

De la desigualdad

$$||f(x_0+h)|-|f(x_0)||\leqslant|f(x_0+h)-f(x_0)|,$$

basada en la fórmula (13) del § 18, y de la continuidad de un polinomio, que acabamos de demostrar, se deduce la *continuidad de módulo* $|f(x)|$ del polinomio $f(x)$; es evidente que este módulo es una función real no negativa de la variable compleja x.

Ahora se demostrarán unos lemas que se empleara en la demostración del teorema fundamental.

Lema sobre el módulo del término superior. *Dado un polinomio de n-ésimo grado, $n\geqslant1$,*

$$f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n$$

de coeficientes complejos arbitrarios, si k es un número real positivo cualquiera, para los valores de la indeterminada x, cuyos módulos son suficientemente grandes, se verifica la desigualdad

$$|a_0x^n|>k|a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n|, \tag{2}$$

es decir, el módulo del término superior es mayor que el módulo de la suma de todos los demás términos, y además, una cantidad arbitraria de veces.

En efecto, sea A el máximo de los módulos de los coeficientes $a_1, a_2, \ldots, a_n$:

$$A = \text{máx}\,(|a_1|, |a_2|, \ldots, |a_n|).$$

Entonces

$$|a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n| \leqslant |a_1|\,|x|^{n-1} + |a_2|\,|x|^{n-2} + \ldots$$
$$\ldots + |a_n| \leqslant A\,(|x|^{n-1} + |x|^{n-2} + \ldots + 1) = A\,\frac{|x|^n - 1}{|x| - 1}.$$

(véase en el § 18 las propiedades de los módulos de la suma y el producto de números complejos).

Suponiendo $|x| > 1$, se obtiene:

$$\frac{|x|^n - 1}{|x| - 1} < \frac{|x|^n}{|x| - 1},$$

de donde

$$|a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n| < A\,\frac{|x|^n}{|x| - 1}.$$

Por lo tanto, se cumplirá la desigualdad (2) si x, además de satisfacer a la condición $|x| > 1$, satisface también a la desigualdad

$$kA\,\frac{|x|^n}{|x| - 1} \leqslant |a_0x^n| = |a_0|\,|x|^n,$$

o sea, si

$$|x| \geqslant \frac{kA}{|a_0|} + 1. \qquad (3)$$

Como el segundo miembro de la desigualdad (3) es mayor que 1, se puede afirmar que para los valores de x que satisfagan a esta desigualdad, se cumple la desigualdad (2), la cual demuestra el lema.

Lema sobre el crecimiento del módulo de un polinomio. *Para todo polinomio $f(x)$ de coeficientes complejos, cuyo grado no sea menor que la unidad, y para cualquier número real positivo M arbitrariamente grande, se puede elegir un número real positivo N tal, que $|f(x)| > M$ para $|x| > N$.*

Sea

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n.$$

En virtud de la fórmula (11) del § 18,

$$|f(x)| = |a_0x^n + (a_1x^{n-1} + \ldots + a_n)| \geqslant$$
$$\geqslant |a_0x^n| - |a_1x^{n-1} + \ldots + a_n|. \qquad (4)$$

Apliquemos el lema sobre el módulo del término superior. Suponiendo $k = 2$, existe un número N_1 tal que

$$|a_0x^n| > 2\,|a_1x^{n-1} + \ldots + a_n|,$$

para $|x| > N_1$.

De aquí que

$$|a_1x^{n-1}+\ldots+a_n|<\frac{1}{2}|a_0x^n|,$$

o sea, en virtud de (4),

$$|f(x)|>|a_0x^n|-\frac{1}{2}|a_0x^n|=\frac{1}{2}|a_0x^n|.$$

El segundo miembro de esta desigualdad será mayor que M para

$$|x|>N_2=\sqrt[n]{\frac{2M}{|a_0|}}.$$

Por lo tanto, $|f(x)|>M$ para $|x|>N=$ máx (N_1, N_2).

Se puede aclarar el significado de este lema mediante la siguiente ilustración geométrica, que se empleará a menudo en este párrafo. Supongamos que por cada punto x_0 del plano complejo se traza una perpendicular a este plano de longitud (referida a la unidad de medida elegida) igual al módulo del valor del polinomio $f(x)$ en este punto, o sea, igual a $|f(x_0)|$. En virtud del teorema de la continuidad del módulo de un polinomio, demostrado anteriormente, los extremos de estas perpendiculares formarán una superficie alabeada continua, situada sobre el plano complejo. El lema sobre el crecimiento del módulo de un polinomio muestra que al aumentar $|x_0|$, esta superficie se aleja más y más del plano complejo, aunque, naturalmente, este alejamiento no es monótono. La fig. 8 representa esquemáticamente la línea de intersección de esta superficie con un plano perpendicular al plano complejo y pasa por el punto O.

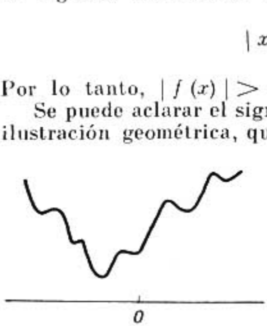

Fig. 8.

En la demostración, el papel fundamental lo desempeña el siguiente lema:

Lema de D'Alembert. *Si para $x=x_0$ el polinomio $f(x)$ de grado n, $n\geqslant 1$, no* se anula, $f(x_0)\neq 0$ y, por lo tanto, $|f(x_0)|>0$, *se puede hallar un incremento h, generalmente complejo*, tal que

$$|f(x_0+h|<|f(x_0)|.$$

Según la fórmula de Taylor, siendo por ahora arbitrario el incremento h, se tiene:

$$f(x_0+h)=f(x_0)+hf'(x_0)+\frac{h^2}{2!}f''(x_0)+\ldots+\frac{h^n}{n!}f^{(n)}(x_0).$$

Por la condición, x_0 no es raíz de $f(x)$. Sin embargo, este número puede ser eventualmente, raíz de $f'(x)$, y también puede ocurrir que sea raíz de ciertas derivadas posteriores. Supongamos que la k-ésima derivada ($k \geqslant 1$) es la primera que no tiene a x_0 por raíz, o sea, que

$$f'(x_0) = f''(x_0) = \ldots = f^{(k-1)}(x_0) = 0, \quad f^{(k)}(x_0) \neq 0.$$

Tal k existe, puesto que si a_0 es el coeficiente superior del polinomio $f(x)$, entonces

$$f^{(n)}(x_0) = n!\, a_0 \neq 0.$$

Por lo tanto

$$f(x_0+h) = f(x_0) + \frac{h^k}{k!} f^{(k)}(x_0) + $$
$$+ \frac{h^{k+1}}{(k+1)!} f^{(k+1)}(x_0) + \ldots + \frac{h^n}{n!} f^{(n)}(x_0).$$

Algunos de los números $f^{(k+1)}(x_0), \ldots, f^{(n-1)}(x_0)$ también pueden ser iguales a cero. Pero esto no importa.

Dividiendo ambos miembros de esta igualdad por $f(x_0)$, que por la condición es diferente de cero, e introduciendo la notación

$$c_j = \frac{f^{(j)}(x_0)}{j!\, f(x_0)}, \quad j = k, \; k+1, \; \ldots, \; n,$$

se obtiene:

$$\frac{f(x_0+h)}{f(x_0)} = 1 + c_k h^k + c_{k+1} h^{k+1} + \ldots + c_n h^n$$

o, puesto que $c_k \neq 0$,

$$\frac{f(x_0+h)}{f(x_0)} = (1 + c_k h^k) + c_k h^k \left(\frac{c_{k+1}}{c_k} h + \ldots + \frac{c_n}{c_k} h^{n-k} \right).$$

Pasando a los módulos se obtiene:

$$\left| \frac{f(x_0+h)}{f(x_0)} \right| \leqslant |1 + c_k h^k| + |c_k h^k| \left| \frac{c_{k+1}}{c_k} h + \ldots + \frac{c_n}{c_k} h^{n-k} \right|. \quad (5)$$

Hasta ahora no hemos hecho ninguna suposición sobre el incremento h. Ahora vamos a **elegir** h; además, elegiremos su módulo y su argumento por separado. El módulo de h se elegirá del modo siguiente. Como

$$\frac{c_{k+1}}{c_k} h + \ldots + \frac{c_n}{c_k} h^{n-k}$$

es un polinomio en h sin término independiente, en virtud del lema 1 $\left(\text{suponiendo } \varepsilon = \frac{1}{2}\right)$, se puede hallar un δ_1 tal que

$$\left| \frac{c_{k+1}}{c_k} h + \ldots + \frac{c_n}{c_k} h^{n-k} \right| < \frac{1}{2}, \quad (6)$$

para $|h| < \delta_1$.

Por otra parte,

$$|c_k h^k| < 1, \quad (7)$$

para

$$|h| < \delta_2 = \sqrt[k]{|c_k|^{-1}}.$$

Supongamos que el módulo de h se ha elegido de acuerdo a la desigualdad

$$|h| < \text{mín}(\delta_1, \ \delta_2). \tag{8}$$

Entonces, en virtud de (6), la desigualdad (5) se convierte en la desigualdad estricta

$$\left|\frac{f(x_0+h)}{f(x_0)}\right| < |1 + c_k h^k| + \frac{1}{2}|c_k h^k|; \tag{9}$$

un poco más adelante utilizaremos la condición (7).

Para la elección del argumento de h, exigiremos que el número $c_k h_k$ sea real y negativo. En otras palabras,

$$\arg(c_k h^k) = \arg c_k + k \arg h = \pi,$$

de donde

$$\arg h = \frac{\pi - \arg c_k}{k}. \tag{10}$$

Con esta elección de h, el número $c_k h^k$ se diferenciará de su valor absoluto en el signo,

$$c_k h^k = -|c_k h^k|;$$

por consiguiente, aplicando la desigualdad (7),

$$|1 + c_k h^k| = |1 - |c_k h^k|| = 1 - |c_k h^k|.$$

En consecuencia, eligiendo h de acuerdo a las condiciones (8) y (10), la desigualdad (9) toma la forma

$$\left|\frac{f(x_0+h)}{f(x_0)}\right| < 1 - |c_k h^k| + \frac{1}{2}|c_k h^k| = 1 - \frac{1}{2}|c_k h^k|,$$

o sea,

$$\left|\frac{f(x_0+h)}{f(x_0)}\right| = \frac{|f(x_0+h)|}{|f(x_0)|} < 1,$$

de donde resulta

$$|f(x_0+h)| < |f(x_0)|,$$

lo que demuestra el lema de D'Alembert.

Mediante la ilustración geométrica que se dio anteriormente, se puede aclarar el lema de D'Alembert del modo siguiente. Supongamos que $|f(x_0)| > 0$. Esto significa que la longitud de la perpendicular al plano complejo, trazada por el punto x_0, es diferente de cero. Entonces, según el lema de D'Alembert, se puede hallar un punto $x_1 = x_0 + h$ tal que $|f(x_1)| < |f(x_0)|$, o sea, la perpendicular en el punto x_1 será más corta que en el punto x_0, y, por consiguiente, la superficie formada por los extremos de las perpendiculares estará en este punto nuevo un poco más cerca del plano complejo. Como se ve por la demostración del lema, el módulo de h se puede suponer lo más pequeño que se desee, o sea, el punto x_1 se puede elegir cuanto más cerca de x_0 se quiera; sin embargo, no aplicaremos a continuación esta observación.

Es evidente que son raíces del polinomio $f(x)$ los números complejos (o sea, los puntos del plano complejo) en los que la superficie formada por los extremos de las perpendiculares está en contacto con este plano. Basándose solamente en el lema de D'Alembert no se puede demostrar la existencia de tales puntos. En efecto, aplicando este lema se puede hallar una sucesión indefinida de puntos x_0, x_1, x_2, . . ., tal que

$$|f(x_0)| > |f(x_1)| > |f(x_2)| > \ldots \tag{11}$$

Sin embargo, de aquí no se deduce la existencia de un punto $\bar{x}$ tal que $f(\bar{x}) = 0$; pues una sucesión decreciente de números reales positivos (11) no tiende necesariamente a cero.

El examen ulterior se basará en un teorema de la teoría de las funciones de la variable compleja que generaliza el teorema de Weierstrass, conocido por el lector en el curso de análisis matemático. Este se refiere a las funciones reales de la variable compleja, es decir, a las funciones de la variable compleja que solamente toman valores reales; un ejemplo de tales funciones es el módulo de un polinomio. En el enunciado de este teorema, para simplificar, se hablará del *círculo cerrado E*, entendiendo por esto un círculo del plano complejo al que se le han añadido todos los puntos de su contorno.

Si una función real $g(x)$ de la variable compleja x es continua en todos los puntos de un círculo cerrado E, en éste existe un punto x_0 tal, que para todos los puntos x de E se verifica la desigualdad $g(x) \geqslant g(x_0)$. Por consiguiente, el valor mínimo de $g(x)$ en el círculo E se alcanza en el punto x_0.

La demostración de este teorema se puede hallar en todos los cursos de teoría de las funciones de la variable compleja, por lo que aquí no se expondrá.

Aclararemos geométricamente este teorema mediante la ilustración empleada anteriormente, limitándonos al caso en que la función $g(x)$ sea no negativa en todos los puntos del círculo E (solamente este caso presenta interés). Tracemos por cada punto x_0 del círculo E una perpendicular de longitud $g(x_0)$. Los extremos de estas perpendiculares formarán un trozo de una superficie alabeada continua, y como el círculo E es cerrado, geométricamente está suficientemente claro que para esta superficie existe un mínimo. Naturalmente, esta ilustración no sustituye a la demostración del teorema.

Ahora podemos pasar a la **demostración directa del teorema fundamental.** Sea dado un polinomio $f(x)$ de grado n, $n \geqslant 1$. Resulta evidente que si su término independiente es a_n, se tiene: $f(0) = a_n$. Apliquemos el lema sobre el crecimiento del módulo de un polinomio, suponiendo $M = |f(0)| = |a_n|$. Por consiguiente, existe un N tal que $|f(x)| > |f(0)|$ para $|x| > N$. Se comprende que la generalización del teorema de Weierstrass indicada anteriormente es aplicable a la función $|f(x)|$ para cualquier círculo cerrado E elegido. Tomemos por E el círculo cerrado, limitado por la circunferencia de radio N con centro en el punto 0. Supongamos que en el círculo E, la función $|f(x)|$ alcanza el mínimo en el punto x_0; entonces, en particular, se tiene: $|f(x_0)| \leqslant |f(0)|$.

Fácilmente se observa que *en todo el plano complejo la función* $|f(x)|$ *alcanza el mínimo en el punto* x_0: si el punto x' está situado fuera de E, se tiene $|x'| > N$, por lo cual,

$$|f(x')| > |f(0)| \geqslant |f(x_0)|.$$

Finalmente, de aquí se deduce que $f(x_0) = 0$, o sea, que x_0 *es raíz de* $f(x)$; si fuese $f(x_0) \neq 0$, entonces, por el lema de D'Alembert, existiría un punto x_1 tal que $|f(x_1)| < |f(x_0)|$; sin embargo, esto contradice a la propiedad del punto x_0 que acabamos de establecer.

En el § 55 se dará otra demostración del teorema fundamental.

§ 24. Consecuencias del teorema fundamental

Sea dado un polinomio de n-ésimo grado, $n \geqslant 1$,

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \tag{1}$$

con cualesquiera coeficientes complejos. De nuevo lo consideramos como una expresión algebraica formal, determinada completamente por el conjunto de sus coeficientes. El teorema fundamental de existencia de la raíz, demostrado en el párrafo anterior, permite afirmar la existencia de una raíz α_1 de $f(x)$, que puede ser real o compleja. Por lo tanto, el polinomio $f(x)$ se puede descomponer en la forma

$$f(x) = (x - \alpha_1)\,\varphi(x).$$

Los coeficientes del polinomio $\varphi(x)$ son de nuevo números reales o complejos y, por consiguiente, $\varphi(x)$ tiene una raíz α_2, de donde,

$$f(x) = (x - \alpha_1)(x - \alpha_2)\,\varphi(x).$$

Continuando de este modo, después de un número finito de operaciones, obtendremos la **descomposición del polinomio** $f(x)$ **de n-ésimo grado en un producto de n factores lineales,**

$$f(x) = a_0 (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n). \tag{2}$$

La causa de la aparición del coeficiente a_0 es la siguiente: si en el segundo miembro de la expresión (2) figurase cierto coeficiente b, después de abrir paréntesis el término superior del polinomio $f(x)$ tendría la forma bx^n, mientras que éste es igual a a_0x^n, en virtud de (1). Por esto, $b = a_0$.

La descomposición (2) del polinomio $f(x)$ es la única descomposición de este tipo, salvo el orden de los factores.

En efecto, supongamos que haya otra descomposición

$$f(x) = a_0(x-\beta_1)(x-\beta_2)\ldots(x-\beta_n). \qquad (3)$$

De (2) y (3) se deduce la igualdad

$$(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) = (x-\beta_1)(x-\beta_2)\ldots(x-\beta_n). \qquad (4)$$

Si la raíz α_i fuese distinta de todas las β_j, $j = 1, 2, \ldots, n$, sustituyendo en (4) α_i en lugar de la indeterminada, obtendríamos cero en el primer miembro, mientras que en el segundo miembro, un número diferente de cero. Por lo tanto, *toda raíz α_i es igual a cierta raíz β_j, y viceversa.*

De aquí todavía no se deduce la identidad de las descomposiciones (2) y (3). En efecto, entre las raíces α_i, $i = 1, 2, \ldots, n$, puede haber iguales entre sí. Supongamos, por ejemplo, que s de estas raíces son iguales a α_1 y que, por otra parte, entre las raíces β_j, $j = 1, 2, \ldots, n$, hay exactamente t iguales a la raíz α_1. Se necesita demostrar que $s = t$.

Como el grado de un producto de polinomios es igual a la suma de los grados de los factores, el producto de dos polinomios diferentes de cero, no puede ser igual a cero. De aquí se deduce que si dos productos de polinomios son iguales entre sí, *ambos miembros de la igualdad se pueden simplificar por el factor común*: si

$$f(x)\,\varphi(x) = g(x)\,\varphi(x)$$

y $\varphi(x) \neq 0$, de la igualdad

$$[f(x) - g(x)]\,\varphi(x) = 0$$

se deduce que

$$f(x) - g(x) = 0,$$

o sea,

$$f(x) = g(x).$$

Apliquemos esto a la igualdad (4). Si, por ejemplo, fuese $s > t$, simplificando ambos miembros de la igualdad (4) por el factor $(x - \alpha_1)^t$, llegaríamos a una igualdad cuyo primer miembro contendría el factor $x - \alpha_1$, mientras que el segundo miembro, no lo contendría. Sin embargo, antes se demostró que esto conduce a una contradicción. Por lo tanto, la unicidad de la descomposición (2) del polinomio $f(x)$ queda demostrada.

Reuniendo todos los factores equivalentes, se puede escribir la descomposición (2) en la forma*

$$f(x) = a_0 (x-\alpha_1)^{k_1} (x-\alpha_2)^{k_2} \dots (x-\alpha_l)^{k_l}, \tag{5}$$

donde

$$k_1 + k_2 + \dots + k_l = n.$$

Aquí se supone que entre las raíces $\alpha_1, \alpha_2, \dots, \alpha_l$ *ya no hay iguales.*

Demostremos que en (5), el *número* k_i, $i = 1, 2, \dots, l$, *es el orden de multiplicidad de la raíz* α_i *del polinomio* $f(x)$. En efecto, si este orden es igual a s_i, entonces, $k_i \leqslant s_i$. Sin embargo, supongamos que $k_i < s_i$. En virtud de la definición del orden de multiplicidad de la raíz, para $f(x)$ subsiste la descomposición

$$f(x) = (x-\alpha_i)^{s_i} \varphi(x).$$

Sustituyendo en esta descomposición el factor $\varphi(x)$ por su descomposición en factores lineales, obtendríamos una descomposición de $f(x)$ en factores lineales, diversa de la descomposición (2), o sea, llegaríamos a una contradicción con la unicidad de esta descomposición, demostrada anteriormente.

Por lo tanto, hemos demostrado el siguiente resultado importante:

Todo polinomio $f(x)$ *de grado* n, $n \geqslant 1$, *de cualesquiera coeficientes numéricos, tiene* n *raíces, contando cada una de las raíces tantas veces como sea su orden de multiplicidad.*

Obsérvese que nuestro teorema subsiste también para $n = 0$, puesto que un polinomio de grado cero, no tiene raíces. Este teorema no se cumple **solamente** para el polinomio 0, el cual no tiene grado alguno y es igual a cero para cualquier valor de x. Esta última observación se utilizará para la demostración del siguiente **teorema:**

Si los polinomios $f(x)$ y $g(x)$ *de grado no superior a* n, *toman valores iguales para más de* n *valores de la indeterminada, entonces* $f(x) = g(x)$.

En efecto, en nuestras condiciones, el polinomio $f(x) - g(x)$ tiene más de n raíces, y como es de grado no superior a n, se cumple la igualdad $f(x) - g(x) = 0$.

Por lo tanto, teniendo en cuenta que hay una infinidad de diversos números, se puede afirmar que *para dos polinomios* $f(x)$ y $g(x)$ *cualesquiera existen tales valores* c *de la indeterminada* x *que* $f(c) \neq g(c)$. Tales c no sólo se pueden hallar entre los números complejos, sino también entre los números reales, entre los racionales e incluso entre los números enteros.

Por consiguiente, **dos polinomios de coeficientes numéricos que tienen diferentes coeficientes, aunque sólo sea en una potencia de la indeterminada** x, *son diversas funciones complejas de la variable compleja* x. Con esto, queda por fin demostrada *para los polinomios*

---

* Se llama descomposición factorial del polinomio $f(x)$. (*Nota del T.*)

de coeficientes numéricos la equivalencia de las dos definiciones de igualdad de los polinomios (la algebraica y la teórico-funcional), indicadas en el § 20.

El teorema demostrado anteriormente permite afirmar que un *polinomio de grado no mayor que n se determina completamente por sus valores para cualesquiera valores distintos de la indeterminada, tomados en cantidad mayor que n.* ¿Pueden ser arbitrarios estos valores del polinomio? Si se supone que se dan los valores del polinomio para $n+1$ valores diversos de la indeterminada, la respuesta es positiva: *siempre existe un polinomio de grado no mayor que n, que tome unos valores prefijados para $n+1$ diversos valores dados de la indeterminada.*

En efecto, supongamos que se necesita hallar un polinomio de grado no mayor que n tal, que para los diferentes valores de la indeterminada $a_1, a_2, \ldots, a_{n+1}$, tome respectivamente los valores $c_1, c_2, \ldots, c_{n+1}$. Este polinomio es:

$$f(x)=\sum_{i=1}^{n+1}\frac{c_i(x-a_1)\ldots(x-a_{i-1})(x-a_{i+1})\ldots(x-a_{n+1})}{(a_i-a_1)\ldots(a_i-a_{i-1})(a_i-a_{i+1})\ldots(a_i-a_{n+1})}. \qquad (6)$$

En efecto, su grado no es mayor que n, y el valor $f(a_i)$ es igual a c_i.

La fórmula (6) se denomina *fórmula de interpolación de Lagrange.* La denominación «de interpolación» se debe a que, conociendo los valores del polinomio en $n+1$ puntos, se pueden hallar por esta fórmula sus valores en cualesquiera otros puntos.

Fórmulas de Vieta. Sea dado un polinomio $f(x)$ de grado n cuyo coeficiente superior es igual a 1:

$$f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n, \qquad (7)$$

y sean $\alpha_1, \alpha_2, \ldots, \alpha_n$ sus raíces*. Entonces la descomposición factorial es

$$f(x)=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n).$$

Multiplicando los paréntesis que figuran en el segundo miembro, reduciendo luego los términos semejantes y comparando los coeficientes obtenidos con los coeficientes de (7), se obtienen las siguientes igualdades, denominadas *fórmulas de Vieta,* que expresan los coeficientes del polinomio mediante sus raíces:

$$\begin{aligned}
a_1&=-(\alpha_1+\alpha_2+\ldots+\alpha_n),\\
a_2&=\alpha_1\alpha_2+\alpha_1\alpha_3+\ldots+\alpha_1\alpha_n+\alpha_2\alpha_3+\ldots+\alpha_{n-1}\alpha_n,\\
a_3&=-(\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\ldots+\alpha_{n-2}\alpha_{n-1}\alpha_n),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_{n-1}&=(-1)^{n-1}(\alpha_1\alpha_2\ldots\alpha_{n-1}+\alpha_1\alpha_2\ldots\alpha_{n-2}\alpha_n+\ldots+\alpha_2\alpha_3\ldots\alpha_n),\\
a_n&=(-1)^n\alpha_1\alpha_2\ldots\alpha_n.
\end{aligned}$$

* Aquí se toma cada raíz múltiple el número respectivo de veces.

Por lo tanto, en el segundo miembro de la k-ésima igualdad, $k = 1, 2, \ldots, n$, figura una suma de todos los productos posibles de k raíces, tomadas con el signo más o menos, según que k sea par o impar.

Para $n = 2$, estas fórmulas se convierten en las relaciones entre las raices y los coeficientes de un polinomio cuadrático, conocidas por el álgebra elemental. Para $n = 3$, o sea, para un polinomio cúbico, estas fórmulas toman la forma:

$$a_1 = -(\alpha_1 + \alpha_2 + \alpha_3), \quad a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \quad a_3 = -\alpha_1\alpha_2\alpha_3.$$

Las fórmulas de Vieta facilitan la escritura del polinomio, conocidas sus raíces. Así, pues, hallemos el polinomio $f(x)$ de cuarto grado, de modo que los números 5 y -2 sean raíces simples y el número 3, raíz múltiple de orden dos. Obtenemos:

$$a_1 = -(5-2+3+3) = -9,$$
$$a_2 = 5\cdot(-2)+5\cdot3+5\cdot3+(-2)\cdot3+(-2)\cdot3+3\cdot3 = 17,$$
$$a_3 = -[5\cdot(-2)\cdot3+5\cdot(-2)\cdot3+5\cdot3\cdot3+(-2)\cdot3\cdot3] = 33,$$
$$a_4 = 5\cdot(-2)\cdot3\cdot3 = -90,$$

por lo cual

$$f(x) = x^4 - 9x^3 + 17x^2 + 33x - 90.$$

Si el coeficiente superior a_0 del polinomio $f(x)$ es diferente de 1, para la aplicación de las fórmulas de Vieta es necesario dividir primero todos los coeficientes por a_0, pues esto no influye en las raíces del polinomio. En este caso, las fórmulas de Vieta dan las expresiones para las razones de todos los coeficientes al coeficiente superior.

Polinomios de coeficientes reales. Ahora se deducirán algunas consecuencias del teorema fundamental del álgebra de los números complejos, referentes a los polinomios de coeficientes reales. Precisamente en estas consecuencias está basada la importancia exclusiva del teorema fundamental antes mencionado.

Supongamos que el polinomio de coeficientes reales

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1} + a_n$$

tiene la raíz imaginaria α, o sea, que

$$a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0.$$

Ya sabemos que no se infringe la última igualdad al sustituir todos los números por los conjugados. Sin embargo, siendo reales todos los coeficientes $a_0, a_1, \ldots, a_{n-1}, a_n$, inclusive el número 0 que figura en el segundo miembro, éstos no se alteran en esta sustitución, obteniéndose la igualdad

$$a_0\overline{\alpha}^n + a_1\overline{\alpha}^{n-1} + \ldots + a_{n-1}\overline{\alpha} + a_n = 0,$$

o sea,

$$f(\bar{\alpha})=0.$$

Por lo tanto, *si un número imaginario α es una raíz de un polinomio $f(x)$ de coeficientes reales, el número conjugado $\bar{\alpha}$ también es una raíz de $f(x)$.*

Por consiguiente, el polinomio $f(x)$ es divisible por el trinomio cuadrático

$$\varphi(x)=(x-\alpha)(x-\bar{\alpha})=x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}, \tag{8}$$

cuyos coeficientes, como ya sabemos por el § 18, son reales. Aplicando esto, demostremos que las *raíces α y $\bar{\alpha}$ del polinomio $f(x)$ son de un mismo orden de multiplicidad.*

En efecto, supongamos que los órdenes de multiplicidad de estas raíces son k y l, y que, por ejemplo, $k>l$. Entonces $f(x)$ es divisible por la l-ésima potencia del polinomio $\varphi(x)$.

$$f(x)=\varphi^l(x)\,q(x).$$

El polinomio $q(x)$, como cociente de dos polinomios de coeficientes reales, también tiene coeficientes reales, pero, en contra de lo demostrado anteriormente, el número α es raíz de éste de orden $(k-l)$, mientras que el número $\bar{\alpha}$ no es raíz. De aquí se deduce que $k=l$.

Por lo tanto, ahora se puede decir que las *raíces imaginarias de todo polinomio de coeficientes reales son conjugadas a pares.* De aquí y de la unicidad de las descomposiciones de la forma (2), demostrada anteriormente, se deduce el siguiente resultado final:

Todo polinomio $f(x)$ de coeficientes reales se descompone de modo único (salvo el orden de los factores) en forma de un producto de su coeficiente superior a_0 y de unos cuantos polinomios de coeficientes reales, unos de los cuales son lineales de la forma $x-\alpha$, correspondientes a sus raíces reales, y otros, son cuadrados de la forma (8), *correspondientes a los pares, de sus raíces imaginarias conjugadas.*

Para lo que sigue, es conveniente subrayar que entre los polinomios de coeficientes reales con el coeficiente superior 1, solamente los polinomios lineales de la forma $x-\alpha$ y los cuadrados de la forma (8), no se descomponen en factores de menor grado o, como diremos, son *irreducibles.*

§ 25. Fracciones racionales

En el curso de análisis matemático, además de las funciones racionales enteras, llamadas polinomios, se estudian también las *funciones racionales fraccionarias*; éstas son los cocientes $\frac{f(x)}{g(x)}$ de dos funciones racionales enteras, donde $g(x)\neq 0$. Con estas funciones se efectúan operaciones algebraicas según las mismas leyes con que se opera con los números racionales, o sea, como con quebrados de numeradores y denominadores enteros. La igualdad de dos funciones racionales fraccionarias o, como en adelante se dirá, de dos *fracciones racionales*, se entenderá también en el mismo sentido que la igualdad de quebrados en la aritmética elemental. Para precisar, consideraremos las fracciones racionales con *coeficientes* reales; el lector observará sin dificultad que todo el contenido del presente párrafo se puede trasladar casi palabra por palabra, al caso de fracciones racionales con coeficientes complejos.

Una fracción racional se llama *irreducible*, si su numerador es primo con su denominador.

Toda fracción racional es igual a una fracción irreducible, determinada unívocamente salvo un factor de grado cero, que es común para el numerador y denominador.

En efecto, cualquier fracción racional se puede simplificar por el máximo común divisor de su numerador y denominador, después de lo cual resulta una fracción irreducible igual a la dada. Después, si las fracciones irreducibles $\frac{f(x)}{g(x)}$ y $\frac{\varphi(x)}{\psi(x)}$ son iguales entre sí, o sea, si

$$f(x)\,\psi(x) = g(x)\,\varphi(x), \tag{1}$$

como $f(x)$ y $g(x)$ son primos entre sí, por la propiedad b) del § 21 se deduce que $\varphi(x)$ es divisible por $f(x)$; y como $\varphi(x)$ y $\psi(x)$ son primos entre sí, resulta que $f(x)$ es divisible por $\varphi(x)$. Por lo tanto, $f(x) = c\varphi(x)$, y de (1) se deduce que $g(x) = c\,\psi(x)$.

Una fracción racional se dice que es *propia*, si el grado del numerador es menor que el grado del denominador. Si convenimos en considerar al polinomio 0 como una fracción propia, subsiste el siguiente **teorema:**

Toda fracción racional se representa de un modo único en forma de una suma de un polinomio y una fracción propia.

En efecto, si se da una fracción racional $\frac{f(x)}{g(x)}$ y si, dividiendo el numerador por el denominador, se obtiene la igualdad

$$f(x) = g(x)\,q(x) + r(x),$$

donde el grado de $r(x)$ es menor que el grado de $g(x)$, entonces, como fácilmente se comprueba,

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}\,.$$

Si también se cumple la igualdad

$$\frac{f(x)}{g(x)} = \bar{q}(x) + \frac{\varphi(x)}{\psi(x)}\,,$$

donde el grado de $\varphi(x)$ es menor que el grado de $\psi(x)$, entonces resulta la igualdad

$$q(x)-\overline{q}(x)=\frac{\varphi(x)}{\psi(x)}-\frac{r(x)}{g(x)}=\frac{\varphi(x)\,g(x)-\psi(x)\,r(x)}{\psi(x)\,g(x)}.$$

Como en el primer miembro figura un polinomio, mientras que en el segundo, una fracción propia, resulta: $q(x)-\overline{q}(x)=0$ y

$$\frac{\varphi(x)}{\psi(x)}-\frac{r(x)}{g(x)}=0.$$

Las fracciones racionales propias pueden ser sometidas a un examen ulterior. Recordemos para esto que, como se ha señalado al final del párrafo anterior, son polinomios reales irreducibles los de la forma $x-\alpha$, donde α es real, y los de la forma $x^2-(\beta+\overline{\beta})\,x+\beta\overline{\beta}$, donde β y $\overline{\beta}$ es un par de números imaginarios conjugados. Como fácilmente se comprueba, en el caso complejo desempeñan un papel análogo los polinomios de la forma $x-\alpha$, donde α es un número complejo cualquiera.

La fracción racional propia $\frac{f(x)}{g(x)}$ se llama *simple*, si su denominador $g(x)$ es una potencia de un polinomio irreducible $p(x)$,

$$g(x)=p^k(x), \qquad k\geqslant 1,$$

y el grado del numerador $f(x)$ es menor que el grado de $p(x)$.

Subsiste también el siguiente **teorema fundamental:**

Toda fracción racional propia se descompone en una suma de fracciones simples.

Demostración. Consideremos primero la fracción racional propia $\frac{f(x)}{g(x)h(x)}$, donde los polinomios $g(x)$ y $h(x)$ son primos entre sí:

$$(g(x),\ h(x))=1.$$

Por consiguiente, en virtud del § 21, existen unos polinomios $\overline{u}(x)$ y $\overline{v}(x)$ tales que

$$g(x)\,\overline{u}(x)+h(x)\,\overline{v}(x)=1.$$

De aquí,

$$g(x)\,[\overline{u}(x)\,f(x)]+h(x)\,[\overline{v}(x)\,f(x)]=f(x). \tag{2}$$

Supongamos que dividiendo el producto $u(x)\,f(x)$ por $h(x)$, se obtiene un resto $u(x)$, cuyo grado es menor que el grado de $h(x)$. En este caso, la igualdad (2) se puede escribir del modo siguiente:

$$g(x)\,u(x)+h(x)\,v(x)=f(x), \tag{3}$$

donde $v(x)$ es un polinomio cuya expresión se podría haber escrito sin dificultad. Como el grado del producto $g(x)\,u(x)$ es menor que el grado del producto $g(x)h(x)$ y esto mismo es cierto, según la condición, para el polinomio $f(x)$, el producto $h(x)\,v(x)$ será también de grado menor que $g(x)\,h(x)$ y, por consiguiente, el grado de $v(x)$ será menor que el grado de $g(x)$. De (3) se deduce ahora la igualdad

$$\frac{f(x)}{g(x)\,h(x)}=\frac{v(x)}{g(x)}+\frac{u(x)}{h(x)},$$

en cuyo segundo miembro figura una suma de fracciones propias.

Si al menos uno de los denominadores $g(x)$, $h(x)$ se descompone en un producto de factores primos entre sí, se puede efectuar la descomposición ulterior; continuando de este modo, se obtiene que *cualquier fracción propia se descompone en una suma de unas cuantas fracciones propias, cada una de las cuales tiene por denominador una potencia de un polinomio irreducible.* Más exactamente, dada una fracción propia $\frac{f(x)}{g(x)}$, cuyo denominador posee la descomposición en factores irreducibles

$$g(x)=p_1^{k_1}(x)\,p_2^{k_2}(x)\,\ldots\,p_l^{k_l}(x)$$

(por supuesto, siempre se puede suponer que el coeficiente superior del denominador de la fracción racional es igual a la unidad), siendo $p_i(x)\neq p_j(x)$ para $i\neq j$, se tiene

$$\frac{f(x)}{g(x)}=\frac{u_1(x)}{p_1^{k_1}(x)}+\frac{u_2(x)}{p_2^{k_2}(x)}+\ldots+\frac{u_l(x)}{p_l^{k_l}(x)};$$

todos los términos del segundo miembro de esta igualdad son fracciones propias.

No queda más que considerar una fracción propia de la forma $\frac{u(x)}{p^k(x)}$, donde $p(x)$ es un polinomio irreducible. Aplicando el algoritmo de la división con resto dividimos $u(x)$ por $p^{k-1}(x)$, luego, el resto obtenido lo dividimos por $p^{k-2}(x)$, etc.

Llegamos a las siguientes igualdades:

$$\begin{aligned} u(x)&=p^{k-1}(x)\,s_1(x)+u_1(x),\\ u_1(x)&=p^{k-2}(x)\,s_2(x)+u_2(x),\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ u_{k-2}(x)&=p(x)\,s_{k-1}(x)+u_{k-1}(x). \end{aligned}$$

Como, por la condición, el grado de $u(x)$ es menor que el grado de $p^k(x)$, y el grado de cada uno de los restos $u_i(x)$, $i=1, 2, \ldots, k-1$, es menor que el grado del divisor correspondiente $p^{k-i}(x)$, los grados de todos los cocientes $s_1(x)$, $s_2(x)$, $\ldots$, $s_{k-1}(x)$ serán estrictamente menores que el grado del polinomio $p(x)$. El grado del último resto $u_{k-1}(x)$ será también menor que el grado de $p(x)$.

De las igualdades obtenidas, resulta:

$$u(x) = p^{k-1}(x)\, s_1(x) + p^{k-2}(x) s_2(x) + \ldots + p(x)\, s_{k-1}(x) + u_{k-1}(x).$$

De aquí, obtenemos la representación buscada de la fracción racional $\frac{u(x)}{p^k(x)}$ en forma de una suma de fracciones simples:

$$\frac{u(x)}{p^k(x)} = \frac{u_{k-1}(x)}{p^k(x)} + \frac{s_{k-1}(x)}{p^{k-1}(x)} + \ldots + \frac{s_2(x)}{p^2(x)} + \frac{s_1(x)}{p(x)}.$$

El teorema fundamental queda demostrado. Este se puede completar con el siguiente **teorema de unicidad:**

Toda fracción racional propia posee una descomposición única en suma de fracciones simples.

En efecto, supongamos que alguna fracción propia se puede expresar de dos modos en forma de una suma de fracciones simples. Restando una de estas expresiones de la otra y reduciendo los términos semejantes, se obtiene una suma de fracciones simples, idénticamente igual a cero. Supongamos que los denominadores de las fracciones simples que forman esta suma son ciertas potencias de diferentes polinomios irreducibles $p_1(x)$, $p_2(x)$, $\ldots$, $p_s(x)$ y sea $p_i^{k_i}(x)$ la potencia superior del polinomio $p_i(x)$, $i=1, 2, \ldots, s$, que figura entre los denominadores. Multiplicando ambos miembros de la igualdad considerada por el producto $p_1^{k_1-1}(x) p_2^{k_2}(x) \ldots p_s^{k_s}(x)$, todos los términos de nuestra suma, menos uno de ellos, se convierten en polinomios. En lo que se refiere al término $\frac{u(x)}{p_1^{k_1}(x)}$, éste se convierte en una fracción cuyo denominador es $p_1(x)$ y cuyo numerador es el producto $u(x) p_2^{k_2}(x) \ldots p_s^{k_s}(x)$. El numerador no se divide exactamente por el denominador, puesto que el polinomio $p_1(x)$ es irreducible y todos los factores del numerador son primos con él. Efectuando la división con resto se obtiene que es igual a cero la suma de un polinomio y una fracción propia diferente de cero, lo cual es imposible.

Ejemplo. Descomponer en una suma de fracciones simples la fracción propia real $\frac{f(x)}{g(x)}$, donde

$$f(x) = 2x^4 - 10x^3 + 7x^2 + 4x + 3,$$
$$g(x) = x^5 - 2x^3 + 2x^2 - 3x + 2.$$

Fácilmente se comprueba que

$$g(x) = (x+2)(x-1)^2(x^2+1),$$

donde cada uno de los polinomios $x+2$, $x-1$, x^2+1, es irreducible. De la teoría que acabamos de exponer se deduce que la descomposición buscada tiene que tener la forma

$$\frac{f(x)}{g(x)}=\frac{A}{x+2}+\frac{B}{(x-1)^2}+\frac{C}{x-1}+\frac{Dx+E}{x^2+1}, \tag{4}$$

donde los números A, B, C, D y E tienen que ser todavía buscados.

De (4) se deduce la igualdad

$$f(x)=A(x-1)^2(x^2+1)+B(x+2)(x^2+1)+C(x+2)(x-1)(x^2+1)+$$
$$+Dx(x+2)(x-1)^2+E(x+2)(x-1)^2. \tag{5}$$

Identificando los coeficientes de iguales potencias de la indeterminada x en ambos miembros de la igualdad (5), obtendríamos un sistema de cinco ecuaciones lineales respecto a cinco incógnitas, A, B, C, D y E; como se deduce de lo demostrado anteriormente, este sistema tiene una solución que además, es única. Sin embargo, procederemos de otro modo.

Poniendo en la igualdad (5) $x=-2$, obtenemos la igualdad, $45A=135$, *de donde*

$$A=3. \tag{6}$$

Poniendo luego en (5) $x=1$, obtenemos, $6B=6$, o sea

$$B=1. \tag{7}$$

Después de esto, ponemos en la igualdad (5) $x=0$ y $x=-1$, sucesivamente. Teniendo en cuenta (6) y (7), obtenemos las ecuaciones

$$\left.\begin{aligned}-2C+2E&=1,\\ -4C-4D+4E&=-8.\end{aligned}\right\} \tag{8}$$

De aquí,

$$D=1. \tag{9}$$

Pongamos, finalmente, en la igualdad (5), $x=2$. Teniendo en cuenta (6), (7) y (9), llegamos a la ecuación

$$20C+4E=-52,$$

que junto con la primera de las ecuaciones (8) da

$$C=-2,\quad E=-3.$$

Por lo tanto,

$$\frac{f(x)}{g(x)}=\frac{3}{x+2}+\frac{1}{(x-1)^2}-\frac{2}{x-1}+\frac{x-3}{x^2+1}.$$

CAPITULO VI

FORMAS CUADRATICAS

§ 26. Reducción de una forma cuadrática a la forma canónica

La teoría de las formas cuadráticas tiene su origen en la geometría analítica, más precisamente, en la teoría de las curvas (y superficies) de segundo orden. Es bien sabido que la ecuación de una curva central de segundo orden en el plano, después de trasladar el origen de coordenadas rectangulares al centro de esta curva, tiene la forma

$$Ax^2 + 2Bxy + Cy^2 = D. \tag{1}$$

Se sabe también que se puede efectuar una rotación de los ejes coordenados en un ángulo α, o sea, un cambio de las coordenadas x, y, por las coordenadas x', y':

$$\left.\begin{aligned} x &= x' \cos\alpha - y' \operatorname{sen}\alpha, \\ y &= x' \operatorname{sen}\alpha + x' \cos\alpha, \end{aligned}\right\} \tag{2}$$

de modo que en las nuevas coordenadas la ecuación de la curva tome la forma «canónica»:

$$A'x'^2 + C'y'^2 = D; \tag{3}$$

por consiguiente, en esta ecuación, el coeficiente del producto $x'y'$ de las indeterminadas es igual a cero. Evidentemente, la transforformación de coordenadas (2) se puede interpretar como una transformación lineal de las indeterminadas (véase el § 13), la cual, además, no es degenerada, puesto que el determinante de sus coeficientes es igual a la unidad. Esta transformación se aplica al primer miembro de la ecuación (1). Por lo tanto, se puede decir que mediante la transformación lineal no degenerada (2), el primer miembro de la ecuación (1) se convierte en el primer miembro de la ecuación (3).

Numerosas aplicaciones reclamaron la elaboración de una teoría análoga para el caso en que el número de las indeterminadas, en lugar de dos, sea igual a cualquier n, y los coeficientes sean, o bien números reales, o bien números complejos cualesquiera.

Generalizando la expresión que figura en el primer miembro de la ecuación (1), llegamos al siguiente concepto.

Se llama *forma cuadrática* f en las n indeterminadas $x_1, x_2, \ldots$ $\ldots, x_n$, a una suma, en la cual cada término o es el cuadrado de una de estas indeterminadas o es el producto de dos indeterminadas diversas. Una forma cuadrática se llama *real* o *compleja* según que sus coeficientes sean números reales o cualesquiera números complejos.

Suponiendo que en la forma cuadrática f ya se ha hecho la reducción de términos semejantes, hagamos las siguientes notaciones para los coeficientes de la misma: el coeficiente de x_i^2 lo designaremos por a_{ii}, y el coeficiente del producto $x_i x_j$, para $i \neq j$, por $2a_{ij}$ (¡compárese con (1)!). Como $x_i x_j = x_j x_i$, el coeficiente de este producto se podría indicar también con la notación $2a_{ji}$, o sea, las notaciones introducidas suponen el cumplimiento de la igualdad:

$$a_{ji} = a_{ij}. \tag{4}$$

El término $2a_{ij}x_i x_j$ se puede escribir ahora en la forma

$$2a_{ij}x_i x_j = a_{ij}x_i x_j + a_{ji}x_j x_i,$$

y toda la forma cuadrática f, en forma de una suma de todos los términos posibles $a_{ij}x_i x_j$, donde i y j, independientemente uno de otro, toman los valores desde 1 hasta n:

$$f = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}x_i x_j; \tag{5}$$

en particular, para $i = j$ resulta el término $a_{ii}x_i^2$.

Con los coeficientes a_{ij} se puede formar, evidentemente, una matriz cuadrada $A = (a_{ij})$ de orden n; ésta se llama *matriz de la forma cuadrática* f, y su rango r, *rango* de esta forma cuadrática. Si, en particular, $r = n$, o sea, si la matriz no es degenerada, la forma cuadrática f también se llama *no degenerada*. En virtud de la igualdad (4), los elementos de la matriz A, simétricos con respecto a la diagonal principal, son iguales entre sí, es decir, la matriz A es *simétrica*. Recíprocamente, para cualquier matriz simétrica A de orden n se puede indicar una forma cuadrática (5) en n indeterminadas, cuyos coeficientes son los elementos de la matriz A.

La forma cuadrática (5) puede ser escrita en otra forma, aplicando el producto de matrices rectangulares, definido en el § 14. Convengamos primero en hacer las siguientes notaciones: dada una matriz cuadrada A, o en general, una matriz rectangular, se designará por A' la matriz que se obtiene transponiendo la matriz A. Si las matrices A y B son tales que está definido su producto, entonces se cumple la igualdad:

$$(AB)' = B'A', \tag{6}$$

o sea, la *matriz transpuesta del producto es igual al producto de las matrices transpuestas de los factores, pero tomadas en orden inverso.*

En efecto, si está definido el producto AB, también estará definido el producto $B'A'$, lo que se comprueba fácilmente: el número de columnas de la matriz B' es igual al número de filas de la matriz A'. El elemento de la matriz $(AB)'$ que figura en su i-ésima fila y en su j-ésima columna, está situado en la matriz AB en la j-ésima fila e i-ésima columna. Por esto, es igual a la suma de los productos de los elementos correspondientes de la j-ésima fila de la matriz A y de la i-ésima columna de la matriz B, o sea, es igual a la suma de los productos de los elementos correspondientes de la j-ésima columna de la matriz A' y de la i-ésima fila de la matriz B'. Con esto, queda demostrada la igualdad (6).

Obsérvese que la *matriz A es simétrica cuando, y sólo cuando, ella coincide con su transpuesta*, o sea, si

$$A' = A.$$

Designemos ahora con X la columna formada por las indeterminadas:

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

X es una matriz de n filas y una columna. Transponiendo esta matriz se obtiene la matriz

$$X' = (x_1, x_2, \ldots, x_n),$$

formada por una sola fila.

La forma cuadrática (5), cuya matriz es $A = (a_{ij})$, se puede escribir ahora en forma del producto:

$$f = X'AX. \tag{7}$$

En efecto, el producto AX es una matriz formada por una columna:

$$AX = \begin{pmatrix} \sum_{j=1}^{n} a_{1j}x_j \\ \sum_{j=1}^{n} a_{2j}x_j \\ \vdots \\ \sum_{j=1}^{n} a_{nj}x_j \end{pmatrix}.$$

Multiplicando por la izquierda esta matriz por la matriz X', se obtiene una matriz», formada por una fila y una columna, que es precisamente el segundo miembro de la igualdad (5).

¿Qué ocurrirá con la forma cuadrática f si se someten las indeterminadas $x_1, x_2, \ldots, x_n$ a una trasformación lineal

$$x_i = \sum_{k=1}^{n} q_{ik} y_k, \qquad i = 1, 2, \ldots, n, \tag{8}$$

de matriz $Q = (q_{ik})$? Se supone que, si la forma f es real, también tienen que ser reales los elementos de la matriz Q. Designando con Y la columna formada por las indeterminadas $y_1, y_2, \ldots, y_n$, escribamos la transformación lineal (8) en forma de una igualdad matricial:

$$X = QY. \tag{9}$$

De aquí, en virtud de (6)

$$X' = Y'Q'. \tag{10}$$

Sustituyendo (9) y (10) en la expresión (7) de la forma f, resulta:

$$f = Y'(Q'AQ)Y,$$

o

$$f = Y'BY,$$

donde

$$B = Q'AQ.$$

La matriz B es simétrica, puesto que, en virtud de la igualdad (6), que se cumple evidentemente para cualquier número de factores, y de la igualdad $A' = A$, que significa que la matriz A es simétrica, se tiene:

$$B' = Q'A'Q = Q'AQ = B.$$

Por lo tanto, queda demostrado el siguiente teorema:

Una forma cuadrática en n indeterminadas de matriz A, después de efectuar una transformación lineal de las indeterminadas de matriz Q, se convierte en una forma cuadrática en las nuevas indeterminadas, siendo la matriz de esta forma el producto $Q'AQ$.

Supongamos ahora que se efectúa una transformación lineal **no degenerada**, o sea, que la matriz Q y, por lo tanto, también la matriz Q', no son degeneradas. En este caso, se obtiene el producto $Q'AQ$ multiplicando la matriz A por unas matrices no degeneradas, por lo cual, como se deduce de los resultados del § 14, el rango de este producto es igual al rango de la matriz A. Por lo tanto, *al efectuar una transformación lineal no degenerada, el rango de la forma cuadrática no se altera.*

Veamos ahora, por analogía con el problema geométrico de la reducción de la ecuación de una curva central de segundo orden a la forma canónica (3), el problema de la reducción de una forma cuadrática arbitraria a la forma de una suma de cuadrados de las indeterminadas, o sea, a una forma en que todos los coeficientes de los productos de diversas indeterminadas sean iguales a cero, realizando para esto una transformación lineal no degenerada; esta forma especial de la forma cuadrática se llama *canónica*. Supongamos primero que, mediante una transformación lineal no degenerada, la forma cuadrática f en n indeterminadas $x_1, x_2, \ldots, x_n$ queda reducida a la forma canónica.

$$f = b_1y_1^2 + b_2y_2^2 + \ldots + b_ny_n^2, \tag{11}$$

donde $y_1, y_2, \ldots, y_n$ son las nuevas indeterminadas. Claro, algunos de los coeficientes $b_1, b_2, \ldots, b_n$ pueden ser iguales a cero. Demostremos que el *número de coeficientes en* (11), *diferentes de cero, es indispensablemente igual al rango r de la forma f.*

En efecto, como hemos llegado a la (11) mediante una transformación no degenerada, la forma cuadrática que figura en el segundo miembro de la igualdad (11) también tiene que ser de rango r. Sin embargo, la matriz de esta forma cuadrática tiene la forma diagonal

$$\begin{pmatrix} b_1 & & & 0 \\ & b_2 & & \\ & & \ddots & \\ 0 & & & b_n \end{pmatrix},$$

y la exigencia de que esta matriz tenga el rango r es equiva ente a la suposición de que en su diagonal principal figuren ex ctamente r elementos diferentes de cero.

Pasemos a la demostración del siguiente **teorema fundamental sobre las formas cuadráticas.**

Toda forma cuadrática puede ser reducida a la forma canónica mediante una transformación lineal no degenerada. Si es que se considera una forma cuadrática real, todos los coeficientes de la transformación lineal indicada se pueden suponer reales.

Este teorema subsiste para el caso de formas cuadrát cas en una indeterminada, puesto que son de la forma ax^2, que ya es canónica. Por consiguiente, podemos hacer la demostración por inducción sobre el número de indeterminadas, es decir, demostrar el teorema para las formas cuadráticas en n indeterminadas, suponiendo que ya está demostrado para las formas de un número menor de indeterminadas.

Sea dada una forma cuadrática

$$f = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j \tag{12}$$

en n indeterminadas $x_1, x_2, \ldots, x_n$. Vamos a procurar hallar una transformación lineal no degenerada de tal modo que separe de f el cuadrado de una de las indeterminadas, o sea, que convierta a f en una suma de este cuadrado y una forma cuadrática en las demás *indeterminadas. Este objetivo se consigue fácilmente cuando entre* los coeficientes $a_{11}, a_{22}, \ldots, a_{nn}$ que figuran en la diagonal principal de la matriz de la forma f haya alguno diferente de cero, o sea, cuando en (12) haya por lo menos un cuadrado de una indeterminada x_i cuyo coeficiente sea diferente de cero.

Sea, por ejemplo, $a_{11} \neq 0$. Entonces, como fácilmente se comprueba, la expresión $a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n)^2$, que representa una forma cuadrática, contiene los mismos términos en la indeterminada x_1 que nuestra forma f y, por lo tanto, la diferencia que

$$f - a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n)^2 = g$$

será una forma cuadrática que contendrá solamente a las indeterminadas $x_2, \ldots, x_n$, pero no a x_1. De aquí, que

$$f = a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n)^2 + g.$$

Haciendo las notaciones

$$y_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n, \quad y_i = x_i \text{ para } i = 2, 3, \ldots, n, \tag{13}$$

se obtiene

$$f = a_{11}^{-1} y_1^2 + g, \tag{14}$$

donde g será ahora una forma cuadrática en las indeterminadas $y_2, y_3, \ldots, y_n$. La expresión (14) es la buscada para la forma f, *puesto que se ha obtenido de (12) mediante una transformación* lineal no degenerada, inversa a la transformación lineal (13), cuyo determinante es a_{11}, lo que implica que no sea degenerada.

Si se cumplen las igualdades $a_{11} = a_{22} = \ldots = a_{nn} = 0$, se debe efectuar previamente una transformación lineal auxiliar que dé lugar a la aparición de cuadrados de las indeterminadas en nuestra forma f. Como entre los coeficientes de la expresión (12) tiene que haber diferentes de cero — en caso contrario no habría que demostrar nada — supondremos que, por ejemplo, $a_{12} \neq 0$, o sea, que f es la suma del término $2a_{12}x_1x_2$ y de otros términos, en cada uno de los cuales figura por lo menos una de las indeterminadas $x_3, \ldots, x_n$.

Hagamos ahora la transformación lineal

$$x_1 = z_1 - z_2, \; x_2 = z_1 + z_2, \; x_i = z_i \text{ para } i = 3, \ldots, n. \tag{15}$$

Esta no es degenerada, puesto que su determinante es:

$$\begin{vmatrix} 1 & -1 & 0 & \ldots & 0 \\ 1 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & \ldots & 1 \end{vmatrix} = 2 \neq 0.$$

Como resultado de esta transformación, el término $2a_{12}x_1x_2$ tomará la forma

$$2a_{12}x_1x_2 = 2a_{12}(z_1 - z_2)(z_1 + z_2) = 2a_{12}z_1^2 - 2a_{12}z_2^2,$$

es decir, en la forma f aparecerán a la vez los cuadrados de dos indeterminadas con coeficientes diferentes de cero, que no podrán simplificarse con los demás términos, puesto que en cada uno de estos últimos hay por lo menos una de las indeterminadas $z_3, \ldots, z_n$. Ahora nos encontramos en las condiciones del caso considerado anteriormente, de modo que con otra transformación lineal más, no degenerada, se podrá reducir la forma f a la forma (14).

Para terminar la demostración no queda más que señalar que la forma cuadrática g depende de un número menor que n de indeterminadas, y por la hipótesis de la inducción, se reduce a la forma canónica mediante una transformación no degenerada de las indeterminadas $y_2, y_3, \ldots, y_n$. Esta transformación, considerada como una transformación (que, como fácilmente se comprueba, no es degenerada) de todas las n indeterminadas, según la cual y_1 se mantiene invariable, reduce (14) a la forma canónica. Por lo tanto, mediante dos o tres transformaciones lineales no degeneradas (que se pueden sustituir por una sola transformación no degenerada: por su producto), la forma cuadrática f se reduce a una suma de cuadrados de las indeterminadas con ciertos coeficientes. Como ya sabemos, el número de estos cuadrados es igual al rango r de la forma. Si además de esto, la forma cuadrática f es real, los coeficientes en la forma canónica de f, así como en la transformación lineal que reduce f a esta forma, serán reales; en efecto, tanto la transformación lineal inversa de (13) como la transformación lineal (15) tienen coeficientes reales.

El teorema queda demostrado fundamental. El método utilizado en esta demostración puede aplicarse en ejemplos concretos para la reducción efectiva de una forma cuadrática a la forma canónica. Pero, en lugar de la inducción que se empleaba en la demostración, se aplica el método expuesto para separar sucesivamente los cuadrados de las indeterminadas.

Ejemplo. Reducir la forma cuadrática

$$f = 2x_1x_2 - 6x_2x_3 + 2x_3x_1. \tag{16}$$

a la forma canónica.

Debido a la ausencia en esta forma de los cuadrados de las indeterminadas, efectuamos primero la transformación lineal no degenerada

$$x_1 = y_1 - y_2, \quad x_1 = y_1 + y_2, \quad x_3 = y_3$$

de matriz

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

después de lo cual se obtiene:

$$f = 2y_1^2 - 2y_2^2 - 4y_1y_3 - 8y_2y_3.$$

Ahora, el coeficiente de y_1^2 es diferente de cero y, por esto, en nuestra forma se puede separar el cuadrado de una indeterminada. Haciendo

$$z_1 = 2y_1 - 2y_3, \quad z_2 = y_2, \quad z_3 = y_3,$$

o sea, efectuando la transformación lineal cuya inversa tiene la matriz

$$B = \begin{pmatrix} \frac{1}{2} & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

la forma f se reduce a la forma

$$f = \frac{1}{2} z_1^2 - 2z_2^2 - 2z_3^2 - 8z_2z_3.$$

Por ahora solamente se ha separado el cuadrado de la indeterminada z_1, puesto que la forma contiene todavía el producto de las otras dos indeterminadas. Aplicando la desigualdad de cero del coeficiente de z_2^2, empleamos de nuevo el método expuesto anteriormente. Efectuando la transformación lineal

$$t_1 = z_1, \quad t_2 = -2z_2 - 4z_3, \quad t_3 = z_3,$$

cuya inversa tiene la matriz

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & -2 \\ 0 & 0 & 1 \end{pmatrix},$$

se reduce, finalmente, *la forma f a la forma canónica*

$$f = \frac{1}{2} t_1^2 - \frac{1}{2} t_2^2 + 6t_3^2. \tag{17}$$

La transformación lineal que reduce simultáneamente la forma (16) a la forma (17) tiene por matriz el producto

$$ABC = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 3 \\ \frac{1}{2} & -\frac{1}{2} & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Mediante una sustitución directa se puede comprobar que la transformación lineal no degenerada $\left(\text{puesto que el determinante es igual a } -\frac{1}{2}\right)$

$$\begin{aligned} x_1 &= \frac{1}{2} t_1 + \frac{1}{2} t_2 + 3t_3, \\ x_2 &= \frac{1}{2} t_1 - \frac{1}{2} t_2 - t_3, \\ x_3 &= \qquad\qquad\quad t_3 \end{aligned}$$

transforma (16) en (17).

La teoría de la reducción de una forma cuadrática a la forma canónica se ha elaborado por analogía con la teoría geométrica de las curvas centrales de segundo orden, pero no puede suponerse que es una generalización de esta última. En efecto, en nuestra teoría se permitía la aplicación de cualesquiera transformaciones lineales no degeneradas, mientras que la reducción de la ecuación de una curva de segundo orden a la forma canónica se consigue aplicando transformaciones lineales de una forma (2) muy especial, que representan rotaciones del plano. Sin embargo, esta teoría geométrica se puede generalizar al caso de formas cuadráticas en n indeterminadas con coeficientes **reales.** En el cap. 8 se hará una exposición de esta generalización, denominada **reducción de las formas cuadráticas a los ejes principales.**

§ 27. Ley de inercia

Generalmente, la forma canónica a que se reduce una forma cuadrática dada no se determina unívocamente, pues toda forma cuadrática se puede reducir a la forma canónica de muchos modos. Así, la forma cuadrática $f = 2x_1x_2 - 6x_2x_3 + 2x_3x_1$, considerada en el párrafo anterior, mediante la transformación lineal no degenerada

$$\begin{aligned} x_1 &= t_1 + 3t_2 + 2t_3, \\ x_2 &= t_1 - t_2 - 2t_3, \\ x_3 &= \qquad t_2 \end{aligned}$$

se reduce a la forma canónica

$$f = 2t_1^2 + 6t_2^2 - 8t_3^2,$$

distinta de la obtenida anteriormente.

Surge la pregunta: ¿Qué tienen de común las diversas formas cuadráticas canónicas a que se reduce la forma f dada? Como veremos, esta cuestión está estrechamente ligada con la siguiente pregunta: ¿cuál es la condición para que una de las dos formas cuadráticas dadas se reduzca a la otra mediante una transformación lineal?

Sin embargo, la respuesta a estas preguntas depende de que sean reales o complejas las formas cuadráticas consideradas.

Supongamos primero que se consideran formas cuadráticas *complejas* arbitrarias y que, a la vez, se permite el empleo de transformaciones lineales no degeneradas también con coeficientes complejos arbitrarios. *Ya sabemos que toda forma cuadrática f en n indeterminadas de rango r*, se reduce a la forma canónica

$$f = c_1 y_1^2 + c_2 y_2^2 + \ldots + c_r y_r^2,$$

donde todos los coeficientes $c_1, c_2, \ldots, c_r$ son diferentes de cero. Teniendo en cuenta que se puede extraer la raíz cuadrada de cualquier número complejo, realicemos la siguiente transformación lineal no degenerada:

$$z_i = \sqrt{c_i}\, y_i \text{ para } i = 1, 2, \ldots, r; \; z_j = y_j \text{ para } j = r+1, \ldots, n.$$

Esta reduce f a la forma

$$f = z_1^2 + z_2^2 + \ldots + z_r^2, \tag{1}$$

denominada *normal*, la cual es, simplemente, la suma de los cuadrados de r indeterminadas con coeficientes iguales a la unidad.

La forma normal depende solamente del rango r de la forma f, es decir, todas las formas cuadráticas de rango r se reducen a una misma forma normal (1). Por consiguiente, si las formas f y g en n indeterminadas son de igual rango r, se puede reducir f a la forma (1), y después, (1) a la forma g, lo que significa que existe una transformación lineal no degenerada que reduce f a la forma g. Por otra parte, como una transformación lineal no degenerada nunca altera el rango de la forma, llegamos al resultado siguiente:

Dos formas cuadráticas complejas en n indeterminadas se reducen una a otra mediante transformaciones lineales no degeneradas con coeficientes complejos cuando, y sólo cuando, éstas son de un mismo rango.

De este teorema se deduce sin dificultad que *puede ser forma canónica de una forma cuadrática compleja de rango r cualquier suma de cuadrados de r indeterminadas con cualesquiera coeficientes complejos diferentes de cero.*

El asunto se complica si se consideran formas cuadráticas **reales** y, sobre todo, si se permiten solamente transformaciones lineales con coeficientes reales, cosa muy importante. En este caso, ya no se puede reducir cualquier forma a la forma (1), puesto que probablemente se tendría que efectuar la extracción de la raíz cuadrada de un número negativo. Sin embargo, si llamamos ahora **forma normal** de una forma cuadrática a la suma de los cuadrados de unas cuantas *indeterminadas, tomadas con los coeficientes* $+1$ *o* -1, se puede demostrar fácilmente, que *cualquier forma cuadrática real f se puede* *reducir a la forma normal mediante una transformación lineal no degenerada con coeficientes reales.*

En efecto, la forma f en n indeterminadas, de rango r, se reduce a la forma canónica, que se puede escribir del modo siguiente (cambiando la numeración de las indeterminadas, si fuese necesario):

$$f = c_1 y_1^2 + \ldots + c_k y_k^2 - c_{k+1} y_{k+1}^2 - \ldots - c_r y_r^2, \qquad 0 \leqslant k \leqslant r,$$

donde todos los números $c_1, \ldots, c_k; c_{k+1}, \ldots, c_r$, son diferentes de cero y positivos. Entonces, la transformación lineal no degenerada con coeficientes reales $z_i = \sqrt{c_i}\, y_i$ para $i = 1, 2, \ldots, r$, $z_j = y_j$ para $j = r+1, \ldots, n$, reduce f a la forma normal,

$$f = z_1^2 + \ldots + z_k^2 - z_{k+1}^2 - \ldots - z_r^2.$$

El número total de cuadrados que figuran aquí es igual al rango de la forma.

Una forma cuadrática real se puede reducir a la forma normal mediante muchas transformaciones diversas, pero salvo el orden de numeración de las indeterminadas ésta se reduce solamente a una forma normal. Esto lo muestra el importante teorema, denominado **ley de inercia de las formas cuadráticas reales:**

El número de cuadrados positivos, así como el número de cuadrados negativos, en la forma normal a que se reduce una forma cuadrática dada con coeficientes reales por una transformación lineal real no degenerada, no depende de la elección de esta transformación.

En efecto, supongamos que una forma cuadrática f de rango r, en n indeterminadas $x_1, x_2, \ldots, x_n$ se ha reducido a la forma normal de dos modos diversos:

$$f = y_1^2 + \ldots + y_k^2 - y_{k+1}^2 - \ldots - y_r^2 =$$
$$= z_1^2 + \ldots + z_l^2 - z_{l+1}^2 - \ldots - z_r^2. \tag{2}$$

Como el paso de las indeterminadas $x_1, x_2, \ldots, x_n$ a las indeterminadas $y_1, y_2, \ldots, y_n$ era una transformación lineal no degenerada, las segundas indeterminadas también se expresarán linealmente mediante las primeras con un determinante diferente de cero:

$$y_i = \sum_{s=1}^{n} a_{is} x_s, \qquad i = 1, 2, \ldots, n. \tag{3}$$

Análogamente

$$z_j = \sum_{t=1}^{n} b_{jt} x_t, \qquad j = 1, 2, \ldots, n, \tag{4}$$

donde el determinante de los coeficientes es de nuevo diferente de cero. Los coeficientes en (3), al igual que en (4), son números reales.

Supongamos ahora que $k < l$, y escribamos el sistema de igualdades:

$$y_1 = 0, \ \ldots, \ y_k = 0, \ z_{l+1} = 0, \ \ldots, \ z_r = 0, \ \ldots, \ z_n = 0. \qquad (5)$$

Si los primeros miembros de estas igualdades se sustituyen por sus expresiones (3) y (4), se obtiene un sistema de $n - l + k$ ecuaciones lineales homogéneas con n incógnitas $x_1, x_2, \ldots, x_n$. El número de ecuaciones en este sistema es menor que el número de incógnitas, por consiguiente, por el § 1, este sistema posee solución real *no nula*, $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Sustituyamos ahora en la igualdad (2) todas las y y todas las z por sus expresiones (3) y (4), y pongamos después en lugar de las indeterminadas los números $\alpha_1, \alpha_2, \ldots, \alpha_n$. Si, para abreviar, se designan con $y_i(\alpha)$ y $z_j(\alpha)$ los valores de las indeterminadas y_i y z_j, que se obtienen después de esta sustitución, la igualdad (2) se convierte, en virtud de (5), en la igualdad

$$-y_{k+1}^2(\alpha) - \ldots - y_r^2(\alpha) = z_1^2(\alpha) + \ldots + z_l^2(\alpha). \qquad (6)$$

Como todos los coeficientes en (3) y (4) son reales, todos los cuadrados que figuran en la igualdad (6) son positivos; por consiguiente, de la igualdad (6) se deduce la igualdad a cero de todos estos cuadrados; de aquí resultan las igualdades:

$$z_1(\alpha) = 0, \ \ldots, \ z_l(\alpha) = 0. \qquad (7)$$

Por otra parte, debido a la misma elección de los números $\alpha_1, \alpha_2, \ldots, \alpha_n$

$$z_{l+1}(\alpha) = 0, \ \ldots, \ z_r(\alpha) = 0, \ \ldots, \ z_n(\alpha) = 0. \qquad (8)$$

Por lo tanto, en virtud de (7) y (8), el sistema de n ecuaciones lineales homogéneas

$$z_i = 0, \ i = 1, 2, \ldots, n,$$

con n incógnitas $x_1, x_2, \ldots, x_n$ posee solución no nula $\alpha_1, \alpha_2, \ldots, \alpha_n$, por lo cual, el determinante de este sistema tiene que ser igual a cero. Sin embargo, esto es absurdo, puesto que se suponía que la transformación (4) era no degenerada. Suponiendo que $l < k$ llegamos también al absurdo. De aquí se deduce la igualdad $k = l$, que demuestra el teorema.

El número de cuadrados positivos en la forma normal a que se reduce una forma cuadrática real f dada, se llama *índice positivo de inercia* de esta forma; el número de cuadrados negativos, *índice negativo de inercia*; y la diferencia entre el índice positivo y el negativo, *signatura* de la forma f. Está claro que dado el rango de la forma, cualquiera de los tres números que acabamos de definir determina completamente a los otros dos y, por esto, en los enunciados que siguen se puede mencionar cualquiera de ellos.

Demostremos ahora el siguiente **teorema:**

Dos formas cuadráticas en n indeterminadas con coeficientes reales se reducen una a otra mediante transformaciones lineales reales no degeneradas cuando, y sólo cuando, tienen el mismo rango y la misma signatura.

En efecto, supongamos que la forma f se reduce a la forma g mediante una transformación real no degenerada. Ya se sabe que esta transformación no altera el rango de la forma. Esta tampoco puede alterar la signatura, puesto que, en caso contrario, las formas f y g se reducirían a diferentes formas normales, y la forma f se reduciría a ambas formas normales, lo cual contradice a la ley de inercia. Recíprocamente, si las formas f y g tienen un mismo rango y una misma signatura, entonces se reducen a una misma forma normal y, en consecuencia, se pueden reducir una a otra.

Si se da una forma cuadrática g en la forma canónica

$$g = b_1y_1^2 + b_2y_2^2 + \ldots + b_ry_r^2, \tag{9}$$

con coeficientes reales diferentes de cero, el rango es, evidentemente, igual a r. Fácilmente se ve, empleando el método aplicado anteriormente de reducción de esa forma a la forma normal, que el índice positivo de inercia de la forma g es igual al número de coeficientes positivos en el segundo miembro de la igualdad (9). De aquí y del teorema anterior se deduce el siguiente resultado:

La forma (9) *será la forma canónica de una forma cuadrática f dada cuando, y sólo cuando, el rango de ésta sea igual a r y su índice positivo de inercia coincida con el número de coeficientes positivos en* (9).

Formas cuadráticas descomponibles. Multiplicando dos formas lineales cualesquiera en n indeterminadas,

$$\varphi = a_1x_1 + a_2x_2 + \ldots + a_nx_n, \quad \psi = b_1x_1 + b_2x_2 + \ldots + b_nx_n,$$

se obtiene, evidentemente, una forma cuadrática. No cualquier forma cuadrática se puede representar en forma de un producto de dos formas lineales, y queremos deducir las condiciones para que esto tenga lugar, o sea, para que la forma cuadrática sea *descomponible*.

Una forma cuadrática compleja $f(x_1, x_2, \ldots, x_n)$ es descomponible cuando, y sólo cuando, su rango es menor o igual a dos. Una forma cuadrática real $f(x_1, x_2, \ldots, x_n)$ es descomponible cuando, y sólo cuando, su rango no es mayor que la unidad, o es igual a dos, pero su signatura es igual a cero.

Examinemos primero el producto de las formas lineales φ y ψ. Si al menos una de estas formas es nula, su producto también será una forma cuadrática con coeficientes nulos, es decir, tendrá el rango 0. Si las formas lineales φ y ψ son proporcionales,

$$\psi = c\varphi,$$

siendo $c \neq 0$, y la forma φ no es nula, supondremos que a_1, por ejemplo, es diferente de cero. Entonces la transformación lineal no degenerada

$$y_1 = a_1x_1 + \ldots + a_nx_n, \quad y_i = x_i \text{ para } i = 2, 3, \ldots, n$$

reduce la forma cuadrática $\varphi\psi$ a la forma

$$\varphi\psi = cy_1^2.$$

Como en el segundo miembro figura una forma cuadrática de rango 1, la forma cuadrática $\varphi\psi$ también tendrá el rango 1. Finalmente, si las formas lineales φ y ψ no son proporcionales, supondremos que

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \neq 0.$$

Entonces la transformación lineal

$$\begin{gathered} y_1 = a_1x_1 + a_2x_2 + \ldots + a_nx_n, \\ y_2 = b_1x_1 + b_2x_2 + \ldots + b_nx_n, \\ y_i = x_i \text{ para } i = 3, 4, \ldots, n \end{gathered}$$

no será degenerada; ésta reducirá la forma cuadrática $\varphi\psi$ a la forma

$$\varphi\psi = y_1y_2.$$

En el segundo miembro figura una forma cuadrática de rango 2, que en el caso de coeficientes reales tendrá la signatura 0.

Pasemos a la demostración de la afirmación recíproca. Por supuesto, una forma cuadrática de rango 0 puede considerarse como el producto de dos formas lineales, una de las cuales es nula. Luego, una forma cuadrática $f(x_1, x_2, \ldots, x_n)$ de rango 1, mediante una transformación lineal no degenerada, se reduce a la forma

$$f = cy_1^2, \quad c \neq 0,$$

o sea, a la forma

$$f = (cy_1)\, y_1.$$

Expresando linealmente y_1 mediante $x_1, x_2, \ldots, x_n$, se obtiene la representación de la forma f en un producto de dos formas lineales. Finalmente, una forma cuadrática real $f(x_1, x_2, \ldots, x_n)$ de rango 2 y signatura 0, mediante una transformación lineal no degenerada, se reduce a la forma

$$f = y_1^2 - y_2^2;$$

a esta misma forma se puede reducir cualquier forma cuadrática compleja de rango 2. Sin embargo,

$$y_1^2 - y_2^2 = (y_1 - y_2)(y_1 + y_2),$$

y en el segundo miembro, después de sustituir y_1 y y_2 por sus expresiones lineales mediante $x_1, x_2, \ldots, x_n$, resultará el producto de dos formas lineales. Así, el teorema queda demostrado.

§ 28. Formas definidas positivas

Una forma cuadrática f en n indeterminadas con coeficientes reales se llama *definida positiva*, si se reduce a una forma normal que consta de n cuadrados positivos, es decir, si tanto el rango como el índice positivo de inercia de esta forma son iguales al número de las indeterminadas.

El siguiente teorema da la posibilidad de caracterizar las formas definidas positivas, sin reducirlas a la forma normal o canónica.

Una forma cuadrática f en n indeterminadas $x_1, x_2, \ldots, x_n$ con coeficientes reales, es definida positiva si, y sólo si, para cualesquiera valores reales de estas indeterminadas, no simultáneamente nulos, la forma toma valores positivos.

Demostración. Supongamos que la forma f es definida positiva, o sea, que se reduce a la forma normal

$$f = y_1^2 + y_2^2 + \ldots + y_n^2, \tag{1}$$

donde

$$y_i = \sum_{j=1}^{n} a_{ij}x_j, \qquad i = 1, 2, \ldots, n, \tag{2}$$

siendo diferente de cero el determinante de los coeficientes reales a_{ij}. Si se quieren poner en f valores reales arbitrarios de las indeterminadas $x_1, x_2, \ldots, x_n$, al menos uno de los cuales es diferente de cero, se pueden ponerlos primero en (2) y, después, los valores obtenidos de y_i, en (1). Obsérvese que los valores obtenidos en (2) para $y_1, y_2, \ldots, y_n$, no pueden ser simultáneamente iguales a cero, puesto que en caso contrario resultaría que el sistema de ecuaciones lineales homogéneas

$$\sum_{j=1}^{n} a_{ij}x_j = 0, \qquad i = 1, 2, \ldots, x,$$

poseería solución no nula a pesar de que su determinante es diferente de cero. Sustituyendo en (1) los valores obtenidos de $y_1, y_2, \ldots, y_n$ se obtiene un valor de la forma f, igual a la suma de los cuadrados de n números reales que no son todos iguales a cero; por consiguiente, este valor es estrictamente positivo.

Recíprocamente, supongamos que la forma f no es definida positiva, o sea, que su rango o su índice positivo de inercia es menor que n. Esto significa que en su forma normal, a la que se reduce mediante una transformación lineal no degenerada (2), el cuadrado de al menos una de las indeterminadas, por ejemplo, de y_n, o bien falta, o bien figura con el signo menos. Demostremos que en este caso se pueden elegir para las indeterminadas $x_1, x_2, \ldots, x_n$ unos valores reales, no todos iguales a cero, de modo que el valor de esta forma para estos valores de las indeterminadas sea igual a cero e incluso negativo. Tales son, por ejemplo, los valores que se obtienen para $x_1, x_2, \ldots, x_n$ al resolver por la regla de Cramer el sistema de ecuaciones lineales que resulta de (2) para $y_1 = y_2 = \ldots = y_{n-1} = 0$, $y_n = 1$. En efecto, para estos valores de las indeterminadas $x_1, x_2, \ldots, x_n$ la forma es igual a cero, si y_n^2 no figura en la forma normal, e igual a -1, si y_n^2 figura en la forma normal con el signo menos.

El teorema que acabamos de demostrar se emplea en todos los casos donde se aplican las formas cuadráticas definidas positivas. Sin embargo, con su ayuda no se puede determinar, valiéndose de los coeficientes de la forma, si ésta es definida positiva o no. Para este fin sirve otro teorema que enunciaremos y demostraremos después de que se introduzca un concepto auxiliar.

Sea dada una forma cuadrática f en n indeterminadas de matriz $A = (a_{ij})$. Los menores de orden $1, 2, \ldots, n$ de esta matriz, situados en el ángulo superior de la izquierda, o sea, los menores

$$a_{11}, \quad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}, \ldots, \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1k} \\ a_{21} & a_{22} & \ldots & a_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ a_{k1} & a_{k2} & \ldots & a_{kk} \end{vmatrix}, \ldots, \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix},$$

el último de los cuales, evidentemente, coincide con el determinante de la matriz A, se llaman *menores principales* de la forma f.

Subsiste el siguiente **teorema:**

Una forma cuadrática f en n indeterminadas con coeficientes reales es definida positiva si, y sólo si, todos sus menores principales son estrictamente positivos.

Demostración. El teorema es cierto para $n = 1$, puesto que en este caso la forma es ax^2 y, por lo tanto, es definida positiva si, y sólo si, $a > 0$. Por esta razón demostraremos el teorema para el caso de n indeterminadas, suponiendo que ya está demostrado para las formas cuadráticas en $n - 1$ indeterminadas.

Hagamos primero la observación siguiente:

Si una forma cuadrática f con coeficientes reales que forman una matriz A, se somete a una transformación lineal no degenerada de matriz real Q, *el signo del determinante de la forma (o sea, del determinante de su matriz) no varía.*

En efecto, después de la transformación se obtiene una forma cuadrática cuya matriz es $Q'AQ$; pero, como $|Q'| = |Q|$, resulta:

$$|Q'AQ| = |Q'| \cdot |A| \cdot |Q| = |A| \cdot |Q|^2,$$

o sea, el determinante $|A|$ se multiplica por un número positivo.

Supongamos ahora que se ha dado una forma cuadrática

$$f=\sum_{i,\,j=1}^{n} a_{ij}x_ix_j.$$

Esta se puede escribir en la forma

$$f=\varphi(x_1, x_2, \ldots, x_{n-1})+2\sum_{i=1}^{n-1} a_{in}x_ix_n+a_{nn}x_n^2, \tag{3}$$

donde φ es una forma cuadrática en $n-1$ indeterminadas, formada por los términos de la forma f que no contienen a la indeterminada x_n. Obsérvese que los menores principales de la forma φ coinciden con todos los menores principales de la forma f, menos con el último.

Supongamos que la forma f es definida positiva. En este caso, la forma φ también será definida positiva, pues si existiesen unos valores de las indeterminadas $x_1, x_2, \ldots, x_n$, no simultáneamente nulos, para los que la forma φ tomase un valor no estrictamente positivo, entonces, poniendo complementariamente $x_n=0$, en virtud de (3), se obtendría también un valor no estrictamente positivo para la forma f, a pesar de que no todos los valores de las indeterminadas $x_1, x_2, \ldots, x_{n-1}, x_n$ son iguales a cero. En consecuencia, según la hipótesis de inducción, todos los menores principales de la forma φ, es decir, todos los menores principales de la forma f, menos el último, son estrictamente positivos. En lo que se refiere al último menor principal de la forma f, o sea, al determinante de la misma matriz A, éste es positivo debido a las razones siguientes: como la forma f es definida positiva, mediante una transformación lineal no degenerada, ésta se reduce a la forma normal que consta de n cuadrados positivos. El determinante de esta forma normal es estrictamente positivo y, por esto, en virtud de la observación hecha anteriormente, es también positivo el determinante de la misma forma f.

Supongamos ahora que todos los menores principales de la forma f son estrictamente positivos. De aquí se deduce que son positivos todos los menores principales de la forma φ, y por la hipótesis de inducción, ésta es definida positiva. Por consiguiente, existe una transformación lineal no degenerada de las indeterminadas $x_1, x_2, \ldots, x_{n-1}$ que reduce la forma φ a una suma de $n-1$ cuadrados positivos de las nuevas indeterminadas $y_1, y_2, \ldots, y_{n-1}$. Esta transformación lineal se puede completar hasta una transformación lineal (no degenerada) de todas las indeterminadas $x_1, x_2, \ldots, x_n$, haciendo $x_n=y_n$. En virtud de (3), mediante la transformación indicada, la forma f se reduce a la forma

$$f=\sum_{i=1}^{n-1} y_i^2+2\sum_{i=1}^{n-1} b_{in}y_iy_n+b_{nn}y_n^2; \tag{4}$$

Las expresiones exactas de los coeficientes b_{in} no tienen interés alguno. Como

$$y_i^2 + 2b_{in}y_iy_n = (y_i + b_{in}y_n)^2 - b_{in}^2y_n^2,$$

en virtud de (4), la transformación lineal no degenerada

$$z_i = y_i + b_{in}y_n, \qquad i = 1,\ 2,\ \ldots,\ n-1,$$
$$z_n = \qquad y_n$$

reduce la forma f a la forma canónica

$$f = \sum_{i=1}^{n-1} z_i^2 + cz_n^2. \tag{5}$$

Para demostrar que la forma f es definida positiva, no queda más que demostrar que el número c es positivo. El determinante de la forma que figura en el segundo miembro de la igualdad (5) es igual a c. Sin embargo, este determinante tiene que ser positivo, puesto que el segundo miembro de la igualdad (5) se ha obtenido de la forma f mediante dos transformaciones lineales no degeneradas, y el determinante de la forma f, como último de los menores principales de ésta, es positivo.

Así, pues, el teorema queda demostrado.

Ejempos. 1. La forma cuadrática

$$f = 5x_1^2 + x_2^2 + 5x_3^2 + 4x_1x_2 - 8x_1x_3 - 4x_2x_3$$

es definida positiva, ya que sus menores principales

$$5, \quad \begin{vmatrix} 5 & 2 \\ 2 & 1 \end{vmatrix} = 1, \quad \begin{vmatrix} 5 & 2 & -4 \\ 2 & 1 & -2 \\ -4 & -2 & 5 \end{vmatrix} = 1$$

son positivos.

2. La forma cuadrática

$$f = 3x_1^2 + x_2^2 + 5x_3^2 + 4x_1x_2 - 8x_1x_3 - 4x_2x_3$$

no es definida positiva, puesto que su segundo menor principal es negativo

$$\begin{vmatrix} 3 & 2 \\ 2 & 1 \end{vmatrix} = -1.$$

Obsérvese que por analogía con las formas cuadráticas definidas positivas se pueden definir las *formas definidas negativas*, o sea, unas formas cuadráticas no degeneradas con coeficientes reales cuyas formas normales contienen solamente cuadrados negativos de las indeterminadas. Las formas cuadráticas degeneradas, cuyas formas normales constan de cuadrados de un mismo signo, se llaman a veces *semidefinidas*. Finalmente, las formas cuadráticas, cuyas formas normales contienen cuadrados de las indeterminadas, tanto positivos como negativos, son *indefinidas*.

CAPITULO VII

ESPACIOS LINEALES

§ 29. Definición del espacio lineal. Isomorfismo

La definición de espacio vectorial de n dimensiones dada en el § 8, comenzaba con la definición de un vector de n dimensiones como un sistema ordenado de n números. Para los vectores de n dimensiones se definieron luego la suma y el producto de ellos por números, lo cual condujo a la noción de espacio vectorial de n dimensiones. Los primeros ejemplos de espacios vectoriales son los conjuntos de vectores-segmentos que parten del origen de coordenadas, en el plano o en el espacio tridimensional. Sin embargo, tratando estos ejemplos en el curso de geometría, no siempre creemos necesario determinar los vectores por sus componentes respecto a un sistema fijo de coordenadas, puesto que la suma de vectores y su producto por un escalar se determinan geométricamente, independientemente de la elección del sistema de coordenadas. Precisamente, la suma de vectores en el plano o en el espacio se efectúa según la regla del paralelogramo y el producto de un vector por un número α significa el alargamiento de este vector en α veces (o la contracción, teniendo que cambiar la dirección del vector por la contraria en caso de que α sea negativo). En el caso general, también es conveniente hacer una definición «sin recurrir a coordenadas» del espacio vectorial, es decir, hacer una definición que no necesite determinar los vectores como sistemas ordenados de números. Ahora se dará tal definición. Esta definición es **axiomática**, pues en ella no se tratará de las propiedades de cada vector por separado, sino que se enumerarán las propiedades que deben poseer las operaciones con los vectores.

Sea dado un conjunto V; sus elementos se designarán con letras latinas minúsculas: a, b, c, . . .*. Supongamos también que en el conjunto V se han definido las operaciones siguientes: *la suma*, que pone en correspondencia a cada par de elementos a, b de V un elemento unívocamente determinado $a + b$ de V, denominado *suma*,

* A diferencia de lo convenido en el capítulo 2, en el presente capítulo y en el siguiente, los vectores se designarán con letras latinas minúsculas, mientras que los números, con letras griegas minúsculas.

y la *multiplicación de un elemento por un número real*, según la cual, el *producto* αa *del elemento* a por el número α está unívocamente determinado y pertenece a V.

Los elementos del conjunto V se llamarán *vectores* y el mismo conjunto V, *espacio lineal* (o *vectorial*, o *afín*) *real*, si las operaciones indicadas poseen las propiedades I—VIII que siguen:

I. La suma es conmutativa, $a + b = b + a$.

II. La suma es asociativa, $(a + b) + c = a + (b + c)$.

III. Existe en V un *elemento nulo* (cero) 0, que satisface a la condición: $a + 0 = a$ para todos los a de V.

Aplicando I, es fácil demostrar la *unicidad del elemento nulo*: si 0_1 y 0_2 son dos elementos nulos, se tiene:

$$0_1 + 0_2 = 0_1, \qquad 0_1 + 0_2 = 0_2 + 0_1 = 0_2,$$

de donde $0_1 = 0_2$.

IV. Para todo elemento a de V existe un *elemento opuesto* $-a$, que satisface a la condición: $a + (-a) = 0$.

Fácilmente se comprueba, en virtud de II y I, la *unicidad del elemento opuesto*: si $(-a)_1$ y $(-a)_2$ son dos elementos opuestos de a, entonces,

$$(-a)_1 + [a + (-a)_2] = (-a_1) + 0 = (-a)_1,$$
$$[(-a)_1 + a] + (-a)_2 = 0 + (-a)_2 = (-a)_2,$$

de donde $(-a)_1 = (-a)_2$.

De los axiomas I—IV se deduce la *existencia y unicidad de la diferencia* $a - b$, o sea, de un elemento que satisface a la ecuación

$$b + x = a. \tag{1}$$

En efecto, se puede poner

$$a - b = a + (-b),$$

pues

$$b + [a + (-b)] = [b + (-b)] + a = 0 + a = a.$$

Si existiese otro elemento más, c, que satisfaciese a la ecuación (1), o sea, que

$$b + c = a,$$

agregando a los dos miembros de esta igualdad el elemento $-b$, resultaría

$$c = a + (-b).$$

Los axiomas V—VIII que siguen (compárese con el § 8), ligan la multiplicación por un número con la suma y con las operaciones sobre los números. Precisamente, para cualesquiera elementos a, b de V, para cualesquiera números reales α, β y para el número real 1, *se tienen que cumplir las igualdades:*

V. $$\alpha (a + b) = \alpha a + \alpha b;$$

VI. $$(\alpha+\beta)\,a=\alpha a+\beta a;$$

VII. $$(\alpha\beta)\,a=\alpha\,(\beta a);$$

VIII. $$1\cdot a=a.$$

Señalemos algunas de las propiedades elementales de estos axiomas:

[1] $$\alpha\cdot 0=0.$$

En efecto, para un a de V,

$$\alpha a=\alpha(a+0)=\alpha a+\alpha\cdot 0,$$

o sea,

$$\alpha\cdot 0=\alpha a-\alpha a=\alpha a+[-(\alpha a)]=0,$$

[2] $$0\cdot a=0,$$

donde en el primer miembro figura el número cero, mientras que en el segundo miembro, el elemento nulo de V.

Para la demostración, tomemos cualquier número α. Entonces

$$\alpha a=(\alpha+0)\,a=\alpha a+0\cdot a,$$

de donde

$$0\cdot a=\alpha a-\alpha a=0.$$

[3]. Si $\alpha a=0$, entonces $\alpha=0$, o bien $a=0$. En efecto, si $\alpha\neq 0$, es decir, que existe el número α^{-1}, entonces

$$a=1\cdot a=(\alpha^{-1}\alpha)\,a=\alpha^{-1}\,(\alpha a)=\alpha^{-1}\cdot 0=0.$$

[4]. $$\alpha\,(-a)=-\alpha a.$$

En efecto,

$$\alpha a+\alpha\,(-a)=\alpha\,[a+(-\alpha)]=\alpha\cdot 0=0,$$

o sea, el elemento $\alpha\,(-a)$ es opuesto al elemento αa.

[5]. $$(-\alpha)\,a=-\alpha a.$$

En realidad,

$$\alpha a+(-\alpha)\,a=[\alpha+(-a)]\,a=0\cdot a=0,$$

o sea, el elemento $(-\alpha)\,a$ es opuesto al elemento αa.

[6]. $$\alpha\,(a-b)=\alpha a-\alpha b.$$

En efecto, en virtud de [4], tendremos

$$\alpha\,(a-b)=\alpha\,[a+(-b)]=\alpha a+\alpha\,(-b)=\alpha a+(-\alpha b)=\alpha a-\alpha b.$$

[7]. $$(\alpha-\beta)\,a=\alpha a-\beta a.$$

Se tiene, en efecto

$$(\alpha-\beta)\,a=[\alpha+(-\beta)]\,a=\alpha a+(-\beta)\,a=\alpha a+(-\beta a)=\alpha a-\beta a.$$

Obsérvese que los axiomas y las consecuencias enumeradas se emplearán a continuación sin reservas especiales.

Antes se dio la definición de espacio lineal real. Suponiendo que en el conjunto V no sólo se ha determinado el producto por números reales, sino también por cualesquiera números complejos, conservando los mismos axiomas I-VIII, se obtiene la definición de *espacio lineal complejo*. Para fijar ideas, se **examinarán a continuación los espacios lineales reales; sin emabargo, todo lo que se diga en el presente capítulo se refiere también palabra por palabra al caso de espacios lineales complejos.**

Es fácil señalar **ejemplos** de espacios lineales reales. Estos son, ante todo, los espacios vectoriales reales de n dimensiones formados por los vectores-filas, que se estudiaron en el cap. 2. También son espacios lineales los conjuntos de vectores-segmentos que parten del origen de coordenadas en el plano o en el espacio tridimensional, si las operaciones de suma y de multiplicación por un número se entienden en el sentido geométrico que se indicó al comienzo de este párrafo.

También existen ejemplos de espacios lineales, como suele decirse, de «infinitas dimensiones». Consideremos todas las sucesiones posibles de números reales; éstas son de la forma

$$a=(\alpha_1\alpha_2, \ldots, \alpha_n, \ldots).$$

Las operaciones con las sucesiones se efectúan componente a componente: si

$$b=(\beta_1, \beta_2, \ldots, \beta_n, \ldots),$$

se tiene

$$a+b=(\alpha_1+\beta_1, \alpha_2+\beta_2, \ldots, \alpha_n+\beta_n, \ldots);$$

por otra parte, para cualquier número real γ,

$$\gamma a=(\gamma\alpha_1, \gamma\alpha_2, \ldots, \gamma\alpha_n, \ldots).$$

Todos los axiomas I—VIII se cumplen, o sea, resulta un espacio lineal real.

Un ejemplo de espacio de infinitas dimensiones es también el conjunto de todas las funciones reales posibles de la variable real, entendiendo por suma de funciones y su producto por un número real lo que está convenido en la teoría de las funciones, es decir, como la suma y el producto por un número de los valores de las funciones para cada valor de la variable independiente.

Isomorfismo. Nuestro objetivo próximo consiste en la elección, entre todos los espacios lineales, de aquellos que naturalmente se pueden llamar espacios de dimensiones finitas. Introduzcamos primero un concepto general.

En la definición de espacio lineal se hablaba de las propiedades de las operaciones sobre los vectores, pero no se decía nada de las propiedades de los mismos vectores. En virtud de esto, puede ocurrir que, aunque los vectores de dos espacios lineales dados sean completamente distintos por su naturaleza, estos dos espacios no se distingan en nada desde el punto de vista de las propiedades de las operaciones. La definición exacta es:

Dos espacios lineales reales V y V' se llaman *isomorfos*, si entre los vectores de los mismos se ha establecido una correspondencia biunívoca —de modo que a cada vector a de V se asocia un vector a' de V', llamado **imagen** del vector a, teniendo que tener diferentes vectores de V diferentes imágenes y teniendo que ser cada vector de V' la imagen de cierto vector de V— y si en esta correspondencia, **la imagen de la suma de dos vectores es la suma de las imágenes de los mismos**

$$(a+b)' = a' + b', \tag{2}$$

y la imagen del producto de un vector por un número es el producto de la imagen de este vector por este mismo número,

$$(\alpha a)' = \alpha a'. \tag{3}$$

Señalemos, que la correspondencia biunívoca entre los espacios V y V' que satisface a las condiciones (2) y (3), se llama *correspondencia de isomorfismo.*

Así, pues, el espacio de los vectores-segmentos en el plano, que parten del origen de coordenadas, es isomorfo al espacio vectorial de dos dimensiones formado por pares ordenados de números reales: se obtiene una correspondencia de isomorfismo entre estos espacios, si en el plano se fija un sistema de coordenadas y a cada vector-segmento se asocia el par ordenado de sus coordenadas.

Demostremos la siguiente propiedad del isomorfismo de los espacios lineales:

en una correspondencia de isomorfismo entre los espacios V y V', la imagen del cero del espacio V es el cero del espacio V'.

En efecto, sea a un vector de V y sea a' su imagen en V'. Entonces, en virtud de (2),

$$a' = (a+0)' = a' + 0',$$

es decir, $0'$ es el cero del espacio V'.

§ 30. Espacios de dimensiones finitas. Bases

Como fácilmente puede comprobar el lector, las dos definiciones de **dependencia lineal** de los vectores-filas que se hicieron en el § 9, así como la demostración de su equivalencia, empleaban solamente las operaciones con los vectores y, por lo tanto, se pueden generalizar para el caso de espacios lineales cualesquiera. Por esta razón, en los espacios lineales definidos axiomáticamente se puede hablar de sistemas de vectores linealmente independientes, de sistemas linealmente independientes máximales (en caso de que existiesen), etc.

Si los espacios lineales V y V' son isomorfos, entonces un sistema de vectores $a_1, a_2, \ldots, a_k$ de V es linealmente dependiente si, y solo si, es linealmente dependiente el sistema de sus imágenes $a'_1, a'_2, \ldots, a'_k$ en V'.

Obsérvese, que si la correspondencia $a \longrightarrow a'$ (para todos los a de V) es una correspondencia de isomorfismo entre V y V', entonces la correspondencia inversa $a' \longrightarrow a$ también es de isomorfismo. Por esto, es suficiente examinar el caso en que el sistema $a_1, a_2, \ldots, a_k$ sea linealmente dependiente. Supongamos que existen unos números $\alpha_1, \alpha_2, \ldots, \alpha_k$, no simultáneamente iguales a cero, tales que

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k = 0.$$

Como ya sabemos, la imagen del segundo miembro de esta igualdad en el isomorfismo considerado es el cero $0'$ del espacio V'. Tomando la imagen del primer miembro y aplicando unas cuantas veces (2) y (3), se obtiene:

$$\alpha_1 a'_1 + \alpha_2 a'_2 + \ldots + \alpha_k a'_k = 0',$$

o sea, el sistema $a'_1, a'_2, \ldots, a'_k$ resulta también linealmente dependiente.

Espacios de dimensiones finitas. Se dice que un espacio lineal V es de *dimensión finita*, si se puede hallar en él un sistema finito de vectores linealmente independiente maximal; cualquier sistema tal de vectores se denominará *base* del espacio V.

Un espacio lineal de dimensión finita puede poseer muchas bases diversas. Así, en el espacio de vectores-segmentos en el plano, cualquier par de vectores, diferentes de cero y no situados en una recta, forma una base. Obsérvese, que nuestra definición de espacio de dimensión finita no responde a la pregunta si pueden existir o no en este espacio bases, compuestas de diferente número de vectores. Incluso, se podría suponer que en algunos espacios de dimensión finita existan bases con un número arbitrariamente grande de vectores. Ahora aclararemos la situación real existente.

Supongamos que el espacio lineal V posee una base

$$e_1, e_2, \ldots, e_n, \tag{1}$$

compuesta de n vectores. Si a es un vector arbitrario de V, como (1) es un sistema linealmente independiente maximal, a se expresa linealmente mediante este sistema:

$$a = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n. \tag{2}$$

Por otra parte, como el sistema (1) es linealmente independiente, la expresión (2) del vector a es única:
si

$$a = \alpha'_1 e_1 + \alpha'_2 e_2 + \ldots + \alpha'_n e_n,$$

se tiene

$$(\alpha_1 - \alpha'_1) e_1 + (\alpha_2 - \alpha'_2) e_2 + \ldots + (\alpha_n - \alpha'_n) e_n = 0,$$

de donde

$$\alpha_i = \alpha'_i, \qquad i = 1, 2, \ldots, n.$$

Por lo tanto, al vector a le corresponde unívocamente la fila

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \tag{3}$$

de los coeficientes de su expresión (2) mediante la base (1) o, como vamos a decir, la *fila de sus coordenadas en la base* (1). Recíprocamente, toda fila de la forma (3), o sea, todo vector de n dimensiones en el sentido del cap. 2, es una fila de coordenadas en la base (1) para cierto vector del espacio V, precisamente para el vector que se expresa en la forma (2) mediante la base (1).

Por consiguiente, hemos obtenido una correspondencia biunívoca entre todos los vectores del espacio V y todos los vectores del espacio vectorial de filas de n dimensiones. Demostremos que esta correspondencia que, naturalmente, depende de la elección de la base (1), es una correspondencia de isomorfismo.

Tomemos también en el espacio V, además del vector a, que se expresa mediante la base (1) en la forma (2), un vector b, cuya expresión mediante la base (1) sea

$$b = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n.$$

Entonces

$$a + b = (\alpha_1 + \beta_1) e_1 + (\alpha_2 + \beta_2) e_2 + \ldots + (\alpha_n + \beta_n) e_n,$$

es decir, *a la suma de los vectores a y b le corresponde la suma de las filas de sus coordenadas en la base* (1). Por otra parte,

$$\gamma a = (\gamma \alpha_1) e_1 + (\gamma \alpha_2) e_2 + \ldots + (\gamma \alpha_n) e_n,$$

o sea, *al producto de un vector a por un número γ le corresponde el producto de la fila de sus coordenadas en la base* (1) *por este mismo número γ.*

Con esto, queda demostrado el teorema siguiente:

Todo espacio lineal que posee una base de n vectores es isomorfo a un espacio vectorial de filas de n dimensiones.

Como ya sabemos, en una correspondencia de isomorfismo entre los espacios lineales, a un sistema de vectores linealmente dependiente le corresponde otro sistema linealmente dependiente, y viceversa; por lo tanto, a un sistema linealmente independiente le corresponde otro sistema linealmente independiente. De aquí se deduce que *en una correspondencia de isomorfismo, a la base le corresponde una base.*

En efecto, supongamos que en una correspondencia de isomorfismo entre los espacios V y V', a la base $e_1, e_2, \ldots, e_n$ del espacio V le corresponde el sistema de vectores $e'_1, e'_2, \ldots, e'_n$ del espacio V' que, aunque sea linealmente independiente, no es maximal. Por consiguiente, en V' se puede hallar un vector f' tal, que el sistema de vectores $e'_1, e'_2, \ldots, e'_n, f'$ se mantenga linealmente independiente. Sin embargo, en el isomorfismo considerado, el vector f' es la imagen de cierto vector f de V. Resulta, entonces, que el sistema de vectores $e_1, e_2, \ldots, e_n, f$ tiene que ser linealmente independiente, lo que contradice a la definición de la base.

Ya sabemos, que en el espacio vectorial de filas de n dimensiones (véase § 9), todos los sistemas linealmente independientes maximales constan de n vectores, que cualquier sistema de $n+1$ vectores es linealmente dependiente y que cualquier sistema de vectores linealmente independiente está contenido en un sistema linealmente independiente maximal. Aplicando las propiedades de las correspondencias de isomorfismo, establecidas anteriormente, llegamos a los resultados siguientes.

Todas las bases de un espacio lineal V de dimensión finita constan de un mismo número de vectores. Si este número es igual a n, V se llama *espacio lineal de n dimensiones* y el número n, *dimensión* de este espacio.

Todo sistema de $n+1$ vectores de un espacio lineal de n dimensiones es linealmente dependiente.

Todo sistema de vectores linealmente independiente de un espacio lineal de n dimensiones está contenido en una base de este espacio.

Ahora, es fácil comprobar que los ejemplos de espacios lineales reales indicados anteriormente, el espacio de sucesiones y el espacio de funciones, no son espacios de dimensión finita, pues, en cada uno de ellos el lector hallará sin dificultad sistemas linealmente independientes que constan de un número de vectores arbitrariamente grande.

Relación entre las bases. El objetivo de nuestro estudio son los espacios lineales de dimensión finita. Se entiende que al estudiar los espacios lineales de n dimensiones, se estudia realmente, el espacio vectorial de filas de n dimensiones que se introdujo en el cap. 2. Sin embargo, en este espacio se había elegido antes una base, en la que todos los vectores del espacio se determinaban por las filas de sus coordenadas; precisamente la base compuesta por los vectores unitarios, o sea, por los vectores que tienen una coordenada igual a la unidad y todas las demás iguales a cero; ahora, todas las bases del espacio son para nosotros equivalentes.

Veamos la cantidad de bases que se pueden hallar en el espacio lineal de n dimensiones y cómo están ligadas estas bases entre sí.

Supongamos que en el espacio lineal V de n dimensiones se han dado las bases

$$e_1,\ e_2,\ \ldots,\ e_n \tag{4}$$

y

$$e'_1,\ e'_2,\ \ldots,\ e'_n. \tag{5}$$

Cada vector de la base (5), del mismo modo que cada vector del espacío V, se expresa unívocamente mediante la base (4),

$$e'_i=\sum_{j=1}^{n}\tau_{ij}e_j,\qquad i=1,\ 2,\ \ldots,\ n. \tag{6}$$

La matriz

$$T=\begin{pmatrix}\tau_{11} & \ldots & \tau_{1n}\\ \cdot & \cdot\ \cdot\ \cdot & \cdot\\ \tau_{n1} & \ldots & \tau_{nn}\end{pmatrix},$$

cuyas filas son filas de las coordenadas de los vectores (5) en la base (4), se denomina *matriz de cambio* de la base (4) por la base (5).

En virtud de (6), la relación entre las bases (4) y (5) y la matriz de cambio T se puede expresar en forma de una igualdad matricial:

$$\begin{pmatrix} e'_1\\ e'_2\\ \cdot\\ \cdot\\ \cdot\\ e'_n\end{pmatrix}=\begin{pmatrix}\tau_{11} & \tau_{12} & \ldots & \tau_{1n}\\ \tau_{21} & \tau_{22} & \ldots & \tau_{2n}\\ \cdot & \cdot & \cdot\ \cdot\ \cdot & \cdot\\ \tau_{n1} & \tau_{n2} & \ldots & \tau_{nn}\end{pmatrix}=\begin{pmatrix} e_1\\ e_2\\ \cdot\\ \cdot\\ \cdot\\ e_n\end{pmatrix} \tag{7}$$

o, en la forma:

$$e'=Te.$$

donde con e y e', se han designado, respectivamente, las bases (4) y (5) escritas en columna.

Por otra parte, si T' es la matriz de cambio de la base (5) por la base (4), se tiene

$$e=T'e'.$$

De aquí

$$e=(T'T)\,e,$$

$$e'=(TT')\,e',$$

y, como las bases e y e' son linealmente independientes, resulta

$$T'T=TT'=E,$$

de donde

$$T'=T^{-1}.$$

Con esto, queda demostrado que *la matriz de cambio de una base por otra es siempre una matriz no degenerada.*

Toda matriz cuadrada no degenerada de orden n con elementos reales es la matriz de cambio de una base dada del espacio lineal real de n dimensiones por otra base.

En efecto, supongamos dada la base (4) y la matriz T, de orden n, no degenerada. Tomemos por (5) el sistema de vectores, para los que las filas de la matriz T son filas de coordenadas en la base (4); por consiguiente, se cumple la igualdad (7). Los vectores (5) son linealmente independientes, puesto que la dependencia lineal entre ellos daría lugar a la dependencia lineal de las filas de la matriz T, lo cual es absurdo, pues T no es degenerada. En consecuencia, el sistema (5), siendo linealmente independiente y constando de n vectores, es una base de nuestro espacio y la matriz T es la matriz de cambio de la base (4) por la base (5).

Vemos, pues, que en el espacio lineal de n dimensiones se pueden hallar tantas bases diversas, cuantas matrices cuadradas diversas no degeneradas de orden n existan. Claro que, en este caso, dos bases que consten de los mismos vectores, pero escritos en orden diverso, se consideran diferentes.

Transformación de las coordenadas de un vector. Supongamos que en el espacio lineal de n dimensiones se han dado las bases (4) y (5) con la matriz de cambio $T=(\tau_{ij})$,

$$e'=Te.$$

Hallemos la relación existente entre las filas de coordenadas de un vector arbitrario a en estas bases.

Supongamos que

$$a=\sum_{j=1}^{n}\alpha_j e_j, \tag{8}$$

$$a=\sum_{i=1}^{n}\alpha'_i e'_i.$$

Aplicando (6), resulta:

$$a=\sum_{i=1}^{n}\alpha'_i\left(\sum_{j=1}^{n}\tau_{ij}e_j\right)=\sum_{j=1}^{n}\left(\sum_{i=1}^{n}\alpha'_i\tau_{ij}\right)e_j.$$

Comparando con (8) y aplicando la unicidad de la expresión de un vector mediante la base, se obtiene:

$$\alpha_j=\sum_{i=1}^{n}\alpha'_i\tau_{ij},\qquad j=1,\ 2,\ \ldots,\ n,$$

o sea, se cumple la igualdad matricial:

$$(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n)=(\alpha'_1,\ \alpha'_2,\ \ldots,\ \alpha'_n)\,T.$$

Por lo tanto, *la fila de coordenadas de un vector a en la base e es igual a la fila de coordenadas de este vector en la base e', multiplicada a la derecha por la matriz de cambio de la base e por la base e'.*

Naturalmente, de aquí se deduce la igualdad

$$(\alpha'_1, \alpha'_2, \ldots, \alpha'_n) = (\alpha_1, \alpha_2, \ldots, \alpha_n)\, T^{-1}.$$

Ejemplo. Examinemos el espacio lineal real de tres dimensiones con la base

$$e_1, e_2, e_3. \tag{9}$$

Los vectores

$$\left.\begin{aligned} e'_1 &= 5e_1 - e_2 - 2e_3,\\ e'_2 &= 2e_1 + 3e_2,\\ e'_3 &= -2e_1 + e_2 + e_3 \end{aligned}\right\} \tag{10}$$

también forman una base en este espacio, siendo

$$T = \begin{pmatrix} 5 & -1 & -2\\ 2 & 3 & 0\\ -2 & 1 & 1 \end{pmatrix},$$

la matriz de cambio de (9) por (10); de donde

$$T^{-1} = \begin{pmatrix} 3 & -1 & 6\\ -2 & 1 & -4\\ 8 & -3 & 17 \end{pmatrix}.$$

Por esto, el vector

$$a = e_1 + 4e_2 - e_3$$

tiene en la base (10) la fila de coordenadas

$$(\alpha'_1, \alpha'_2, \alpha'_3) = (1, 4, -1)\begin{pmatrix} 3 & -1 & 6\\ -2 & 1 & -4\\ 8 & -3 & 17 \end{pmatrix} = (-13, 6, -27),$$

o sea,

$$a = -13e'_1 + 6e'_2 - 27e'_3.$$

§ 31. Transformaciones lineales

Ya nos encontramos en el cap. 3 con el concepto de transformación lineal de las indeterminadas. El concepto que se va a introducir ahora lleva el mismo nombre, pero tiene diferente carácter. Ahora bien, se pueden indicar ciertas relaciones entre estos dos conceptos homónimos.

Sea dado un espacio lineal real de n dimensiones, que lo designaremos con V_n. Examinemos una *transformación* de este espacio, o sea, una correspondencia que asocia **a cada** vector a del espacio V_n cierto vector a' de este mismo espacio. El vector a' se llama *imagen* del vector a en la transformación considerada.

Si la transformación se designa con φ, convendremos en designar la imagen del vector a con $a\varphi$ y no con $\varphi(a)$ o φa, como es usual para el lector. Por lo tanto

$$a' = a\varphi.$$

Una transformación φ del espacio lineal V_n se denomina *transformación lineal* de este espacio, si ésta transforma la suma de dos vectores cualesquiera a, b en la suma de las imágenes de estos vectores,

$$(a+b)\,\varphi = a\varphi + b\varphi, \tag{1}$$

y el producto de cualquier vector a por cualquier número α, en el producto de la imagen del vector a por este mismo número α,

$$(\alpha a)\,\varphi = \alpha\,(a\varphi). \tag{2}$$

De esta definición resulta inmediatamente que *la transformación lineal del espacio lineal transforma cualquier combinación lineal de los vectores dados a_1, a_2, ..., a_k en la combinación lineal (con los mismos coeficientes) de las imágenes de estos vectores*:

$$(\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k)\,\varphi = \alpha_1\,(a_1\varphi) + \alpha_2\,(a_2\varphi) + \ldots + \alpha_k\,(a_k\varphi). \tag{3}$$

Demostremos la siguiente afirmación:

Para cualquier transformación lineal φ del espacio lineal V_n, el vector nulo 0 se mantiene inmóvil,

$$0\varphi = 0,$$

y la imagen del vector opuesto al vector dado a, es el vector opuesto a la imagen del vector a,

$$(-a)\,\varphi = -a\varphi.$$

En efecto, si b es un vector arbitrario, en virtud de (2), se tiene

$$0\varphi = (0\cdot b)\,\varphi = 0\cdot(b\varphi) = 0.$$

Por otra parte,

$$(-a)\,\varphi = [(-1)\,a]\,\varphi = (-1)\,(a\varphi) = -a\varphi.$$

El concepto de transformación lineal de un espacio lineal surgió como una generalización de la transformación afín del plano o del espacio de tres dimensiones, tratada en el curso de geometría analítica; en efecto, las condiciones (1) y (2) para las transformaciones afines se cumplen. Estas condiciones también se cumplen para las proyecciones de los vectores en el plano o para las proyecciones sobre una recta (o sobre un plano) en el espacio de tres dimensiones. Por lo tanto, en el espacio lineal de dos dimensiones, de vectores-segmentos que parten del origen de coordenadas en el plano, la transformación de cualquier vector en su proyección sobre un eje que pase por el origen de coordenadas, es una transformación lineal.

Son ejemplos de transformaciones lineales en un espacio arbitrario V_n, la *transformación idéntica* ε, que mantiene a cada vector a en su sitio,

$$a\varepsilon = a,$$

y la *transformación nula* ω, que transforma cualquier vector a en el vector nulo,

$$a\omega = 0.$$

Estudiemos ahora todas las transformaciones lineales del espacio V_n. Sea

$$e_1,\ e_2,\ \ldots,\ e_n \tag{4}$$

una base de este espacio; igual que antes, la base (4), colocada en columna, se designará con e. Como cualquier vector a del espacio V_n se representa unívocamente en forma de una combinación lineal de los vectores de la base (4), la imagen del vector a, en virtud de (3), se expresa mediante las imágenes de los vectores (4) con los mismos coeficientes. En otras palabras, *toda transformación lineal φ del espacio V_n se determina unívocamente por las imágenes $e_1\varphi$, $e_2\varphi$, ..., $e_n\varphi$ de todos los vectores de una base* (4) *fijada.*

Cualquiera que sea el sistema de n vectores ordenados

$$c_1,\ c_2,\ \ldots,\ c_n, \tag{5}$$

del espacio V_n, existe una transformación lineal de este espacio y sólo una, tal que el sistema (5) *es el sistema de imágenes de los vectores de la base* (4) *en esta transformación,*

$$e_1\varphi = c_i, \qquad i = 1,\ 2,\ \ldots,\ n. \tag{6}$$

La unicidad de la transformación φ se demostró anteriormente y sólo queda por demostrar su existencia. Determinemos una transformación φ del modo siguiente: si a es un vector arbitrario del espacio y

$$a = \sum_{i=1}^{n} \alpha_i e_i$$

es su expresión en la base (4), supondremos que

$$a\varphi = \sum_{i=1}^{n} \alpha_i c_i. \tag{7}$$

Demostremos que esta transformación es lineal. Si

$$b = \sum_{i=1}^{n} \beta_i e_i$$

es cualquier otro vector del espacio, se tiene

$$(a+b)\varphi = \Big[\sum_{i=1}^{n} (\alpha_i+\beta_i)e_i\Big]\varphi = \sum_{i=1}^{n} (\alpha_i+\beta_i)\,c_i =$$
$$= \sum_{i=1}^{n} \alpha_i c_i + \sum_{i=1}^{n} \beta_i c_i = a\varphi + b\varphi.$$

Si γ es un número cualquiera, entonces

$$(\gamma a)\varphi = \Big[\sum_{i=1}^{n} (\gamma a_i)\,e_i\Big]\varphi = \sum_{i=1}^{n} (\gamma\alpha_i)\,c_i = \gamma \sum_{i=1}^{n} \alpha_i c_i = \gamma\,(a\varphi).$$

En lo que se refiere a la igualdad (6), ésta se cumple debido a la definición (7) de la transformación φ, puesto que todas la coordenadas del vector e_i en la base (4) son iguales a cero, excepto la i-ésima coordenada, que es igual a la unidad.

Por consiguiente, hemos establecido una correspondencia biunívoca entre todas las transformaciones del espacio lineal V_n y todos los sistemas ordenados (5) *formados por n vectores de este espacio.*

Sin embargo, todo vector c_i posee una determinada expresión en la base (4),

$$c_i = \sum_{j=1}^{n} \alpha_{ij} e_j, \qquad i = 1, 2, \ldots, n. \tag{8}$$

Con las coordenadas del vector c_i en la base (4) se puede formar una matriz cuadrada

$$A = (\alpha_{ij}) \tag{9}$$

tomando por i-ésima fila la fila de coordenadas del vector c_i, $i = 1, 2, \ldots, n$. Como el sistema (5) es arbitrario, la matriz A será una matriz cuadrada arbitraria de orden n con elementos reales.

Por lo tanto, resulta una correspondencia biunívoca entre todas las transformaciones lineales del espacio V_n y todas las matrices cuadradas de orden n; por supuesto, esta correspondencia depende de la elección de la base (4).

Se dice que la matriz A *determina* la transformación lineal φ en la base (4), o, abreviadamente, que A es *la matriz de la transformación lineal* φ en la base (4). Si designamos con $e\varphi$ la columna formada por las imágenes de los vectores de la base (4), entonces, de (6), (8) y (9) se deduce la siguiente igualdad matricial, que describe totalmente la relación existente entre la transformación lineal φ, la base e y la matriz A que determina esta transformación lineal en esta base:

$$e\varphi = Ae. \tag{10}$$

He aquí cómo se hallan las coordenadas de la imagen $a\varphi$ del vector a en la base (4), conociendo las coordenadas del mismo vector

a en la misma base y la matriz A de la transformación lineal φ. Si

$$a = \sum_{i=1}^{n} \alpha_i e_i,$$

se tiene

$$a\varphi = \sum_{i=1}^{n} \alpha_i (e_i\varphi),$$

lo que es equivalente a la igualdad matricial

$$a\varphi = (\alpha_1, \alpha_2, \ldots, \alpha_n)(e\varphi).$$

Aplicando (10) y teniendo en cuenta que la multiplicación de las matrices es asociativa también cuando una de las matrices es una columna formada por vectores (lo cual fácilmente se comprueba), resulta:

$$a\varphi = [(\alpha_1, \alpha_2, \ldots, \alpha_n) A] e.$$

De aquí se deduce que *la fila de coordenadas del vector $a\varphi$ es igual a la fila de coordenadas del vector a, multiplicada a la derecha por la matriz A de la transformación lineal, todo efectuado en la base* (4).

Ejemplo. Supongamos que en la base e_1, e_2, e_3 del espacio lineal de tres dimensiones, la transformación lineal se da mediante la matriz

$$A = \begin{pmatrix} -2 & 1 & 0 \\ 1 & 3 & 2 \\ 0 & -4 & 1 \end{pmatrix}.$$

Si

$$a = 5e_1 + e_2 - 2e_3,$$

entonces

$$(5, 1, -2)\begin{pmatrix} -2 & 1 & 0 \\ 1 & 3 & 2 \\ 0 & -4 & 1 \end{pmatrix} = (-9, 16, 0),$$

o sea,

$$a\varphi = -9e_1 + 16e_2.$$

Relación entre las matrices de una transformación lineal en diversas bases. Naturalmente, la matriz que determina la transformación lineal depende de la elección de la base. Hallemos la relación entre las matrices que determinan una misma transformación lineal pero en bases diferentes.

Sean dadas las bases e y e' con la matriz de cambio T,

$$e' = Te, \tag{11}$$

y supongamos que la transformación lineal φ se determina en estas bases por las matrices A y A', respectivamente,

$$e\varphi = Ae, \quad e'\varphi = A'e'. \tag{12}$$

En virtud de (11), la segunda de las igualdades (12) da lugar a la igualdad

$$(Te)\varphi = A'(Te).$$

Pero

$$(Te)\varphi = T(e\varphi).$$

En efecto, si $(\tau_{i1}, \tau_{i2}, \ldots, \tau_{in})$ es la i-ésima fila de la matriz T, se tiene

$$(\tau_{i1}e_1 + \tau_{i2}e_2 + \ldots + \tau_{in}e_n)\varphi = \tau_{i1}(e_1\varphi) + \tau_{i2}(e_2\varphi) + \ldots + \tau_{in}(e_n\varphi).$$

Por lo tanto, en virtud de (12),

$$(Te)\varphi = T(e\varphi) = T(Ae) = (TA)e,$$
$$A'(Te) = (A'T)e,$$

o sea,

$$(TA)e = (A'T)e.$$

Si al menos para un i, $1 \leqslant i \leqslant n$, la i-ésima fila de la matriz TA fuese diferente de la i-ésima fila de la matriz $A'T$, entonces dos distintas combinaciones lineales de los vectores $e_1, e_2, \ldots, e_n$ resultarían iguales entre sí, lo cual es absurdo, puesto que la base e es linealmente independiente. Por lo tanto,

$$TA = A'T,$$

y como la matriz de cambio T no es degenerada, de aquí resulta que

$$A' = TAT^{-1}, \quad A = T^{-1}A'T. \tag{13}$$

Dos matrices, B y C, se llaman *semejantes*, si están ligadas por la igualdad

$$C = Q^{-1}BQ,$$

donde Q es una matriz no degenerada. En este caso, se dice que la matriz C es la *transformada* de la matriz B por la matriz Q.

Por lo tanto, las igualdades (13) demostradas anteriormente se pueden enunciar en forma del siguiente importante **teorema:**

Las matrices que determinan una misma transformación lineal en diferentes bases, son semejantes entre sí. Además, la matriz de la transformación lineal φ en la base e' se obtiene transformando la matriz de esta transformación en la base e por la matriz de cambio de la base e' a la base e.

Subrayemos que, si la matriz A determina la transformación φ en la base e, cualquier matriz B semejante a la matriz A,

$$B = Q^{-1}AQ,$$

también determina la transformación φ en cierta base, precisamente, en la base que se obtiene de la base e mediante la matriz de cambio Q^{-1}.

Operaciones con las transformaciones lineales. Como ya se demostró, asociando a cada transformación lineal del espacio V_n su matriz en una base fija, resulta una correspondencia biunívoca entre todas las transformaciones lineales y todas las matrices cuadradas de orden n. Es natural esperar que a las operaciones de adición y multiplicación de las matrices, y también a la multiplicación de una matriz por un número, les correspondan unas operaciones análogas con las transformaciones lineales.

Sean dadas en el espacio V_n las transformaciones φ y ψ. Llamemos *suma* de estas transformaciones a la transformación $\varphi+\psi$, determinada por la igualdad

$$a(\varphi+\psi)=a\varphi+a\psi; \tag{14}$$

por consiguiente, ésta transforma cualquier vector a en la suma de sus imágenes en las transformaciones φ y ψ.

La transformación $\varphi+\psi$ es lineal. En efecto, para cualesquiera vectores a y b y cualquier número α,

$$(a+b)(\varphi+\psi)=(a+b)\varphi+(a+b)\psi=$$
$$=a\varphi+b\varphi+a\psi+b\psi=a(\varphi+\psi)+b(\varphi+\psi);$$
$$(\alpha a)(\varphi+\psi)=(\alpha a)\varphi+(\alpha a)\psi=\alpha(a\varphi)+\alpha(a\psi)=$$
$$=\alpha(a\varphi+a\psi)=\alpha[a(\varphi+\psi)].$$

Por otra parte, llamemos *producto* de las transformaciones lineales φ y ψ a la transformación $\varphi\psi$ determinada por la igualdad

$$a(\varphi\psi)=(a\varphi)\psi, \tag{15}$$

es decir, que se obtiene como resultado de la realización sucesiva de las transformaciones φ y ψ.

La transformación $\varphi\psi$ es lineal:

$$(a+b)(\varphi\psi)=[(a+b)\varphi]\psi=(a\varphi+b\varphi)\psi=$$
$$=(a\varphi)\psi+(b\varphi)\psi=a(\varphi\psi)+b(\varphi\psi);$$
$$(\alpha a)(\varphi\psi)=[(\alpha a)\varphi]\psi=[\alpha(a\varphi)]\psi=\alpha[(a\varphi)\psi]=\alpha[a(\varphi\psi)].$$

Finalmente, llamemos *producto de la transformación lineal* φ *por el número* $\varkappa$ a la transformación $\varkappa\varphi$ determinada por la igualdad

$$a(\varkappa\varphi)=\varkappa(a\varphi); \tag{16}$$

de aquí que en la transformación φ las imágenes de todos los vectores se multiplican por el número $\varkappa$.

La transformación $\varkappa\varphi$ es lineal:

$$(a+b)(\varkappa\varphi)=\varkappa[(a+b)\varphi]=\varkappa(a\varphi+b\varphi)=$$
$$=\varkappa(a\varphi)+\varkappa(b\varphi)=a(\varkappa\varphi)+b(x\varphi);$$
$$(\alpha a)(\varkappa\varphi)=\varkappa[(\alpha a)\varphi]=\varkappa[\alpha(a\varphi)]=\alpha[\varkappa(a\varphi)]=\alpha[a(\varkappa\varphi)].$$

Supongamos que en la base $e_1, e_2, \ldots, e_n$, las transformaciones φ y ψ se determinan por las matrices $A = (\alpha_{ij})$ y $B = (\beta_{ij})$, respectivamente,

$$e\varphi = Ae, \quad e\psi = Be.$$

Entonces, en virtud de (14),

$$e_i(\varphi+\psi) = e_i\varphi + e_i\psi = \sum_{j=1}^{n} \alpha_{ij}e_j + \sum_{j=1}^{n} \beta_{ij}e_j = \sum_{j=1}^{n} (\alpha_{ij}+\beta_{ij})\, e_j,$$

o sea

$$e(\varphi+\psi) = (A+B)\, e.$$

Por lo tanto, *la matriz de la suma de transformaciones lineales en cualquier base es igual a la suma de las matrices de estas transformaciones en esta misma base.*

Por otra parte, en virtud de (15),

$$e_i(\varphi\psi) = (e_i\varphi)\,\psi = \left(\sum_{j=1}^{n} \alpha_{ij}e_j\right)\psi = \sum_{j=1}^{n} \alpha_{ij}(e_j\psi) =$$

$$= \sum_{j=1}^{n} \alpha_{ij}\left(\sum_{k=1}^{n} \beta_{jk}e_k\right) = \sum_{k=1}^{n}\left(\sum_{j=1}^{n} \alpha_{ij}\beta_{jk}\right) e_k,$$

o sea,

$$e(\varphi\psi) = (AB)\, e.$$

En otras palabras, *la matriz del producto de transformaciones lineales en cualquer base es igual al producto de las matrices de estas transformaciones en la misma base.*

Finalmente, en virtud de (16),

$$e_i(\varkappa\varphi) = \varkappa(e_i\varphi) = \varkappa \sum_{j=1}^{n} \alpha_{ij}e_j = \sum_{j=1}^{n} (\varkappa\alpha_{ij})\, e_j,$$

o sea,

$$e(\varkappa\varphi) = (\varkappa A)\, e.$$

Por consiguiente, *la matriz que determina en cierta base el producto de la transformación lineal φ por el número $\varkappa$, es igual al producto de la matriz de la misma transformación φ en esta base por el número $\varkappa$.*

De los resultados obtenidos se deduce que las operaciones con las transformaciones lineales poseen las mismas propiedades que las operaciones con las matrices. Así, pues, la suma de transformaciones lineales es conmutativa y asociativa, y el producto es asociativo, aunque para $n > 1$ no es conmutativo. Para las transformaciones lineales existe la resta unívoca. Obsérvese también que *entre las trans-*

formaciones lineales, la transformación idéntica ε desempeña el papel de la unidad, y la transformación nula ω, el papel del cero. En efecto, en cualquier base, la transformación ε se determina por la matriz unidad, y la transformación ω, por la matriz nula.

§ 32. Subespacios lineales

Un subconjunto L del espacio lineal V se llama *subespacio lineal* de este espacio, si él mismo es un espacio lineal con respecto a las operaciones de suma de vectores y de multiplicación de un vector por un número, determinadas en V. Así, pues, en el espacio euclídeo de tres dimensiones, el conjunto de vectores que parten del origen de coordenadas y que están situados en un plano (o en una recta) que pasa por el origen, es un subespacio lineal.

Para que un subconjunto no vacío L del espacio V sea un subespacio lineal de éste, es suficiente que se cumplan las condiciones siguientes:

1. *Si los vectores a y b pertenecen a L, el vector $a+b$ también pertenece a L.*
2. *Si el vector a pertenece a L, el vector αa también pertenece a L para cualquier valor del número α.*

En efecto, en virtud de la condición 2, el conjunto L contiene el vector nulo, pues, si el vector a pertenece a L, el vector $0\cdot a=0$ también pertenece a L. Luego, junto con cada uno de sus vectores a, y otra vez en virtud de la condición 2, el vector opuesto $-a = (-1)\cdot a$ también pertenece a L, por lo cual, debido a la condición 1, también pertenece a L la diferencia de dos vectores cualesquiera de L. En lo que se refiere a las demás condiciones incluidas en la definición del espacio lineal, cumpliéndose éstas en V, también se cumplen en L.

Pueden servir de ejemplos de subespacios lineales del espacio V, el mismo espacio V, así como el conjunto compuesto del solo vector nulo, denominado *subespacio nulo*. De mayor interés es el siguiente: tomemos en el espacio V cualquier sistema finito de vectores

$$a_1,\ a_2,\ \ldots,\ a_r \tag{1}$$

y designemos con L el conjunto de todos los vectores que son combinaciónes lineales de los vectores (1). Demostremos que L es un subespacio lineal. En efecto, si

$$b=\alpha_1a_1+\alpha_2a_2+\ldots+\alpha_ra_r,\quad c=\beta_1a_1+\beta_2a_2+\ldots+\beta_ra_r,$$

se tiene

$$b+c=(\alpha_1+\beta_1)\,a_1+(\alpha_2+\beta_2)\,a_2+\ldots+(\alpha_r+\beta_r)\,a_r,$$

o sea, el vector $b+c$ pertenece a L; también pertenece a L el vector

$$\gamma b = (\gamma\alpha_1) a_1 + (\gamma\alpha_2) a_2 + \ldots + (\gamma\alpha_r) a_r$$

para cualquier número γ.

Suele decirse que este subespacio lineal L *está engendrado* por el sistema de vectores (1); en particular, los mismos vectores (1) pertenecen a L.

Por cierto, *todo subespacio lineal de un espacio lineal de dimensión finita se engendra por un sistema finito de vectores*, ya que, si el subespacio no es el nulo, posee incluso una base finita. La dimensión del subespacio lineal L no es mayor que la dimensión n del mismo espacio V_n, siendo igual a n solamente cuando $L = V_n$. Evidentemente, la dimensión del subespacio nulo se debe tomar igual a cero.

Para cualquier k, $0 < k < n$, en el espacio V_n existen subespacios lineales de dimensión k; para esto, es suficiente considerar el subespacio engendrado por cualquier sistema de k vectores linealmente independientes.

Supongamos que en el espacio V se han dado los subespacios lineales L_1 y L_2. Como fácilmente se comprueba, el conjunto de vectores L_0 que pertenecen simultáneamente a L_1 y a L_2, es un subespacio lineal; éste se llama *intersección* de los subespacios L_1 y L_2. Por otra parte, también es un subespacio lineal la suma $\overline{L}$ de los subespacios L_1 y L_2, o sea, el conjunto de todos los vectores de V que se representan en forma de una suma de dos vectores, uno de los cuales pertenece a L_1 y el otro, a L_2. Si d_1, d_2, d_0 y $\overline{d}$ son las dimensiones respectivas de los subespacios L_1, L_2, L_0 y $\overline{L}$, se cumple la igualdad:

$$\overline{d} = d_1 + d_2 - d_0, \tag{2}$$

es decir, *la dimensión de la suma de dos subespacios es igual a la suma de las dimensiones de estos subespacios menos la dimensión de su intersección.*

Para la demostración, se toma una base arbitraria

$$a_1, a_2, \ldots, a_{d_0} \tag{3}$$

del subespacio L_0 y se completa hasta que se forme una base

$$a_1, a_2, \ldots, a_{d_0}, b_{d_0+1}, \ldots, b_{d_1} \tag{4}$$

del subespacio L_1, y hasta que se forme una base

$$a_1, a_2, \ldots, a_{d_0}, \quad c_{d_0+1}, \ldots, c_{d_2} \tag{5}$$

del subespacio L_2. Aplicando la definición del subespacio $\overline{L}$, se observa sin dificultad que éste se engendra por el sistema de vectores

$$a_1, a_2, \ldots, a_{d_0}, b_{d_0+1}, \ldots, b_{d_1}, c_{d_0+1}, \ldots, c_{d_2}. \tag{6}$$

Por consiguiente, la fórmula (2) quedará demostrada si se demuestra que el sistema (6) es linealmente independiente.

Supongamos que se cumple la igualdad

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_{d_0} a_{d_0} + \beta_{d_0+1} b_{d_0+1} + \ldots + \beta_{d_1} b_{d_1} + \\ + \gamma_{d_0+1} c_{d_0+1} + \ldots + \gamma_{d_2} c_{d_2} = 0$$

con ciertos coeficientes numéricos. Entonces,

$$d = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_{d_0} a_{d_0} + \beta_{d_0+1} b_{d_0+1} + \ldots + \beta_{d_1} b_{d_1} = \\ = -\gamma_{d_0+1} c_{d_0+1} - \ldots - \gamma_{d_2} c_{d_2}. \quad (7)$$

El primer miembro de esta igualdad pertenece a L_1, el segundo, a L_2. Por consiguiente, el vector d, que es igual tanto al primer miembro como al segundo miembro de esta igualdad, pertenece a L_0, por lo cual se expresa linealmente mediante la base (3). Sin embargo, el segundo miembro de la igualdad (7) muestra que el vector d también se expresa linealmente mediante los vectores $c_{d_0+1}, \ldots, c_{d_2}$. Como el sistema (5) es linealmente independiente, resulta que todos los coeficientes $\gamma_{d_0+1}, \ldots, \gamma_{d_2}$ son iguales a cero, es decir, $d = 0$, y por lo tanto, como el sistema (4) es linealmente independiente, también son iguales a cero todos los coeficientes $\alpha_1, \ldots, \alpha_{d_0}, \beta_{d_0+1}, \ldots, \beta_{d_1}$. Con esto, queda demostrada la independencia lineal del sistema (6).

Se recomienda al lector comprobar que nuestra demostración es válida también para el caso en que el subespacio L_0 sea nulo, o sea, $d_0 = 0$.

Campo de valores y núcleo de una transformación lineal. Supongamos que en el espacio lineal V_n es dada una transformación lineal φ. De las definiciones de subespacio lineal y de tranformación lineal se deduce inmediatamente que si L es un subespacio lineal cualquiera del espacio V_n, **el conjunto $L\varphi$ de las imágenes de todos los vectores de L en la transformación φ también es un subespacio lineal**; en particular, el conjunto $V_n\,\varphi$ de las imágenes de todos los vectores del espacio V_n es también un subespacio lineal; este conjunto se llama *campo de valores* de la transformación φ.

Hallemos la dimensión del campo de valores. Para esto, obsérvese que, como todas las matrices que determinan la transformación φ en diferentes bases son semejantes entre sí, todas ellas tienen un mismo rango en virtud del último teorema del § 14. Por consiguiente, este número puede recibir el nombre de *rango* de la transformación lineal φ.

La dimensión del campo de valores de una transformación lineal φ es igual al rango de esta última.

En efecto, *supongamos que* φ *se determina en la base* e_1, e_2, . . ., e_n por la matriz A. El subespacio $V_n\varphi$ se engendra por los vectores

$$e_1\varphi,\ e_2\varphi,\ \ldots,\ e_n\varphi \tag{8}$$

y, en particular, cualquier subsistema linealmente independiente, maximal del sistema (8) será base del subespacio $V_n\varphi$. Pero, el maximo número de vectores linealmente independientes del sistema (8) es igual al máximo número de filas linealmente independientes de la matriz A, es decir, es igual al rango de esta matriz. El teorema queda demostrado.

Ya sabemos que en una transformación lineal φ, el vector nulo *se transforma en sí mismo. El conjunto* N (φ) *de todos los vectores* del espacio V_n que se transforman en el vector nulo en la transformación φ, no es, pues, vacío, y es, evidentemente, un subespacio lineal. Este subespacio se denomina *núcleo* de la transformación φ, y su dimensión lleva el nombre de *defecto* de la misma.

Para cualquier transformación lineal φ *del espacio* V_n, *la suma del rango y del defecto de la misma es igual a la dimensión* n *de todo el espacio.*

En efecto, si r es el rango de la transformación φ, el subespacio $V_n\varphi$ posee una base de r vectores

$$a_1,\ a_2,\ \ldots,\ a_r. \tag{9}$$

En el espacio V_n se pueden elegir tales vectores

$$b_2,\ b_2,\ \ldots,\ b_r, \tag{10}$$

que

$$b_i\varphi = a_i, \qquad i = 1,\ 2,\ \ldots,\ r;$$

evidentemente, la elección de los vectores (10) no es única. Si alguna combinación lineal no trivial de los vectores (10) se transformase en cero y, en particular, si los vectores (10) fuesen linealmente dependientes, los vectores (9) también resultarían linealmente dependientes, en contra de la suposición. Por esto, el subespacio lineal L engendrado por los vectores (10), tiene la dimensión r, y su intersección con el subespacio N (φ) es igual a cero.

Por otra parte, la suma de los subespacios L y N (φ) coincide con todo el espacio V_n. En efecto, siendo c cualquier vector del espacio, el vector $d = c\varphi$ pertenece, naturalmente, al subespacio $V_n\varphi$. Entonces, existe en el subespacio L un vector b tal que

$$b\varphi = d;$$

el vector b se expresa mediante el sistema (10) con los mismos coeficientes con que se expresa el vector d mediante la base (9). Por consiguiente

$$c = b + (c - b).$$

donde el vector $c-b$ pertenece al subespacio $N(\varphi)$, puesto que

$$(c-b)\varphi = c\varphi - b\varphi = d - d = 0.$$

La afirmación del teorema se deduce de los resultados obtenidos y de la fórmula (2).

Transformaciones lineales no degeneradas. Una transformación lineal φ del espacio lineal V_n se llama *no degenerada*, si se satisface cualquiera de las condiciones siguientes, cuya equivalencia es consecuencia inmediata de los teoremas demostrados anteriormente:

1. **El rango de la transformación φ es igual a n.**
2. **El campo de valores de la transformación φ es todo el espacio V_n.**
3. **El defecto de la transformación φ es igual a cero.**

Para las transformaciones lineales no degeneradas se pueden dar también muchas otras definiciones equivalentes a las señaladas y, en particular, las definiciones 4—6 que siguen.

4. **Diferentes vectores del espacio V_n tienen en la transformación φ diferentes imágenes.**

En efecto, si la transformación φ posee la propiedad 4, el núcleo de esta transformación consta solamente del vector nulo, o sea, se cumple también la condición 3. Si los vectores a y b son tales que $a \neq b$, pero $a\varphi = b\varphi$, se tiene $a-b \neq 0$, pero $(a-b)\varphi = 0$, es decir, no se cumple la condición 3.

De 2 y 4 se deduce:

5. **La transformación φ es una correspondencia biunívoca del espacio V_n sobre todo este espacio.**

De 5 se deduce que, para una transformación lineal φ no degenerada, existe la *transformación inversa* φ^{-1} que transforma cada vector $a\varphi$ en el vector a,

$$(a\varphi)\varphi^{-1} = a.$$

La transformación φ^{-1} es lineal, puesto que

$$(a\varphi + b\varphi)\varphi^{-1} = [(a+b)\varphi]\varphi^{-1} = a + b,$$
$$[\alpha(a\varphi)]\varphi^{-1} = [(\alpha a)\varphi]\varphi^{-1} = \alpha a.$$

De la definición de la transformación φ^{-1}, se deduce que

$$\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon; \tag{11}$$

las mismas igualdades (11) se pueden considerar como la definición de la transformación inversa. De aquí y de los últimos resultados del párrafo anterior, se deduce que *si una transformación lineal φ no degenerada se determina en cierta base por la matriz A, que no es degenerada en virtud de la propiedad 1, entonces la transformación φ^{-1} se determina en esta base por la matriz A^{-1}.*

Por lo tanto, llegamos a la siguiente definición de transformación lineal no degenerada:

6. **Para la transformación φ existe la transformación lineal inversa φ^{-1}.**

§ 33. Raíces características y valores propios

Sea $A = (\alpha_{ij})$ una matriz cuadrada de orden n con elementos reales. Sea, por otra parte, λ una indeterminada. Entonces la matriz $A-\lambda E$, donde E es la matriz unidad de orden n, se llama *matriz característica* de la matriz A. Como en la diagonal principal de la matriz λE, figura λ, siendo iguales a cero todos los demás elementos, resulta

$$A-\lambda E=\begin{pmatrix} \alpha_{11}-\lambda & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22}-\lambda & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn}-\lambda \end{pmatrix}.$$

El determinante de la matriz $A-\lambda E$ es un polinomio en λ, de orden n. En efecto, el producto de los elementos que figuran en la diagonal principal es un polinomio en λ con el término superior $(-1)^n\lambda^n$. Todos los demás términos del determinante no contienen al menos dos de los elementos que figuran en la diagonal principal, por lo que su grado respecto a λ no es mayor que $n-2$. Los coeficientes de este polinomio se podrían hallar fácilmente. Así, pues, el coeficiente de λ^{n-1} es igual a $(-1)^{n-1}(\alpha_{11}+\alpha_{22}+\dots+\alpha_{nn})$ *y el término independiente coincide con el determinante de la matriz* A.

El polinomio de n-ésimo grado $|A-\lambda E|$ se llama *polinomio característico* de la matriz A, y sus raíces, que pueden ser tanto reales como imaginarias, se llaman *raíces características* de la misma.

Las matrices semejantes poseen iguales polinomios característicos y, por consiguiente, iguales raíces características.

En efecto, supongamos que

$$B=Q^{-1}AQ.$$

Entonces, teniendo en cuenta que la matriz λE es conmutable con la matriz Q y que $|Q^{-1}|=|Q|^{-1}$, resulta:

$$|B-\lambda E|=|Q^{-1}AQ-\lambda E|=|Q^{-1}(A-\lambda E)Q|=$$
$$=|Q|^{-1}\cdot|A-\lambda E|\cdot|Q|=|A-\lambda E|,$$

que es lo que se quería demostrar.

En virtud del teorema demostrado en el § 31 sobre la relación entre las matrices que determinan una transformación lineal en diferentes bases, se deduce que *a pesar de que la transformación lineal φ se puede determinar por diferentes matrices en bases diversas, sin embargo, estas matrices tienen un mismo conjunto de raíces características*. Por consiguiente, estas raíces se pueden llamar *raíces características de la misma transformación* φ. Todo el conjunto de estas raíces características, tomando cada raíz con el mismo orden de multiplicidad que tiene en el polinomio característico, se llama *espectro* de la transformación lineal φ.

Las raíces características desempeñan un gran papel en el estudio de las transformaciones lineales. El lector tendrá muchas oportunidades para convencerse de esto. Por ahora, indicaremos una de las aplicaciones de las raíces características.

Supongamos que en el espacio lineal real V_n se ha dado una transformación lineal φ. Si en este caso el vector b, diferente de cero, se transforma en otro que es proporcional al mismo vector b,

$$b\varphi=\lambda_0 b, \tag{1}$$

donde λ_0 es cierto número real, el vector b se llama *vector propio* de la transformación φ y el número λ_0, *valor propio* de la misma; además, se dice que el vector propio b *corresponde* al valor propio λ_0.

Obsérvese que como $b\neq 0$, el número λ_0 que satisface a la condición (1) se determina para el vector b unívocamente. Subrayemos luego que el vector nulo no se considera vector propio de la transformación φ, a pesar de que satisface a la condición (1) para cualquier λ_0.

La rotación del plano euclídeo alrededor del origen de coordenadas, en un ángulo que no sea múltiplo de π es un ejemplo de transformación lineal que carece de vectores propios. Otro ejemplo de caso extremo es la dilatación del plano; aquí todos los vectores que parten del origen de coordenadas se alargan, aumentando de longitud por ejemplo, cinco veces. Para esta transformación lineal, son propios todos los vectores no nulos del plano; todos ellos corresponden al valor propio 5.

Las raíces características reales de la transformación lineal φ, (si es que éstas existen), y sólo éstas, son valores propios de la misma.

En efecto, supongamos que en la base $e_1, e_2, \ldots, e_n$, la transformación φ tiene la matriz $A=(\alpha_{ij})$ y sea

$$b=\sum_{i=1}^{n}\beta_i e_i$$

un vector propio de la transformación φ,

$$b\varphi=\lambda_0 b.$$

Como se ha demostrado en el § 31,

$$b\varphi=[(\beta_1,\ \beta_2,\ \ldots,\ \beta_n)\,A]\,e. \tag{3}$$

Las igualdades (2) y (3) dan lugar al sistema de igualdades

$$\left.\begin{array}{l}\beta_1\alpha_{11}+\beta_2\alpha_{21}+\ldots+\beta_n\alpha_{n1}=\lambda_0\beta_1,\\ \beta_1\alpha_{12}+\beta_2\alpha_{22}+\ldots+\beta_n\alpha_{n2}=\lambda_0\beta_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ \beta_1\alpha_{1n}+\beta_2\alpha_{2n}+\ldots+\beta_n\alpha_{nn}=\lambda_0\beta_n.\end{array}\right\} \tag{4}$$

Como $b \neq 0$, no todos los números $\beta_1, \beta_2, \ldots, \beta_n$ son iguales a *cero*. Por lo tanto, en virtud de (4), *el sistema de ecuaciones* lineales homogéneas

$$\begin{aligned} (\alpha_{11} - \lambda_0) x_1 + \alpha_{21} x_2 + \ldots + \alpha_{n1} x_n &= 0, \\ \alpha_{12} x_1 + (\alpha_{22} - \lambda_0) x_2 + \ldots + \alpha_{n2} x_n &= 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha_{1n} x_1 + \alpha_{2n} x_2 + \ldots + (\alpha_{nn} - \lambda_0) x_n &= 0 \end{aligned} \tag{5}$$

posee solución no nula; de donde su determinante es igual a cero,

$$\begin{vmatrix} \alpha_{11} - \lambda_0, & \alpha_{21}, & \ldots, & \alpha_{n1} \\ \alpha_{12}, & \alpha_{22} - \lambda_0, & \ldots, & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n}, & \alpha_{2n}, & \ldots, & \alpha_{nn} - \lambda_0 \end{vmatrix} = 0. \tag{6}$$

Transponiendo, resulta

$$|A - \lambda_0 E| = 0, \tag{7}$$

o sea, el valor propio λ_0 es, en efecto, raíz característica de la matriz A y, por consiguiente, de la transformación φ; naturalmente, éste es real.

Recíprocamente, supongamos que λ_0 es una raíz característica real cualquiera de la transformación φ y, por consiguiente, de la matriz A. Entonces, se cumple la igualdad (7) y, por lo tanto, también la igualdad (6) obtenida de la (7) por transposición. De aquí se deduce que el sistema de ecuaciones lineales homogéneas (5) posee solución no nula, e incluso real, puesto que todos los coeficientes de este sistema son reales. Indicando esta solución mediante

$$(\beta_1, \beta_2, \ldots, \beta_n), \tag{8}$$

se verifican las igualdades (4). Designemos con b el vector del espacio V_n que tiene la fila de coordenadas (8) en la base $e_1, e_2, \ldots, e_n$; está claro que $b \neq 0$. Entonces, se verifica la igualdad (3), y de (4) y (3) *se deduce* (2). *Por lo tanto, resulta que b es un vector propio* de la transformación φ, correspondiente al valor propio λ_0. El teorema queda demostrado.

Obsérvese que si se examinase un espacio lineal complejo, no habría necesidad de que la raíz característica fuese real, o sea, quedaría demostrado el teorema siguiente: *las raíces características de una transformación lineal del espacio lineal complejo, y sólo ellas, son valores propios de esta transformación*. De aquí se deduce que *toda transformación lineal posee vectores propios en el espacio lineal complejo*.

Volviendo al caso real considerado, señalemos que el conjunto de los vectores propios de la transformación lineal φ que corresponden al valor propio λ_0, coincide con el conjunto de soluciones reales no nulas del sistema de ecuaciones lineales homogéneas (5). De aquí se deduce que *el conjunto de vectores propios de la transformación lineal* φ, *correspondientes al valor propio* λ_0, *después de agregarle el vector nulo, es un subespacio lineal del espacio* V_n. En efecto, de lo demostrado en el § 12 se deduce que *el conjunto de las soluciones (reales) de cualquier sistema de ecuaciones lineales homogéneas con* n *incógnitas es un subespacio lineal del espacio* V_n.

Transformaciones lineales con espectro simple. En muchos casos se necesita saber si una transformación lineal dada φ puede tener en cierta base una matriz diagonal. En realidad, no cualquier transformación lineal se puede determinar por una matriz diagonal. En el § 61 se indicarán las condiciones necesarias y suficientes para esto; ahora queremos exponer una condición suficiente.

Demostremos primero las siguientes proposiciones auxiliares:

Una transformación lineal φ *se determina en la base* $e_1, e_2, \ldots, e_n$ *por una matriz diagonal cuando, y sólo cuando, todos los vectores de esta base son vectores propios de la transformación* φ.

En efecto, la igualdad

$$e_i\varphi = \lambda_i e_i$$

equivale a que en la i-ésima fila de la matriz que determina la transformación lineal en la base indicada, sean iguales a cero todos los elementos que estén fuera de la diagonal principal, y que en la diagonal principal (o sea, en el i-ésimo lugar) figure el número λ_i.

Los vectores propios $b_1, b_2, \ldots, b_k$ *de la transformación lineal* φ *que corresponden a diferentes valores propios, forman un sistema linealmente independiente.*

Demostraremos esta afirmación por el método de inducción sobre k, puesto que para $k=1$ se cumple: un vector propio, diferente de cero, forma un sistema linealmente independiente. Supongamos que

$$b_i\varphi = \lambda_i b_i, \quad i = 1, 2, \ldots, k,$$

donde

$$\lambda_i \neq \lambda_j \text{ para } i \neq j.$$

Si existiese una dependencia lineal

$$\alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_k b_k = 0, \tag{9}$$

donde, por ejemplo, $\alpha_1 \neq 0$, entonces aplicando a ambos miembros de la igualdad (9) la transformación φ, obtendríamos

$$\alpha_1\lambda_1 b_1 + \alpha_2\lambda_2 b_2 + \ldots + \alpha_k\lambda_k b_k = 0.$$

Restando de aquí la igualdad (9) multiplicada por λ_k, resultaría

$$\alpha_1(\lambda_1-\lambda_k)\,b_1+\alpha_2(\lambda_2-\lambda_k)\,b_2+\ldots+\alpha_{k-1}(\lambda_{k-1}-\lambda_k)\,b_{k-1}=0,$$

lo que da una dependencia lineal no trivial entre los vectores $b_1, b_2, \ldots, b_{k-1}$, pues $\alpha_1(\lambda_1-\lambda_k)\neq 0$.

Se dice que una transformación lineal φ del espacio lineal real V_n tiene un *espectro simple*, si todas sus raíces características son reales y distintas. Por consiguiente, la transformación φ tiene n valores propios distintos, de aquí que, en virtud del teorema demostrado, en el espacio V_n existe una base compuesta de vectores propios de esta transformación. Por lo tanto, *toda transformación lineal con espectro simple puede determinarse por una matriz diagonal.*

Pasando de la transformación lineal a las matrices que la determinan, obtenemos el resultado siguiente:

Toda matriz cuyas raíces características son reales y distintas, es semejante a una matriz diagonal o, como suele decirse, se reduce a la forma diagonal.

CAPITULO VIII

ESPACIOS EUCLIDEOS

§ 34. Definición del espacio euclídeo. Bases ortonormales

El concepto de espacio lineal de n dimensiones no generaliza en gran medida el concepto de plano euclídeo o de espacio euclídeo de tres dimensiones, pues, en el caso de n dimensiones, para $n > 3$ no está definida ni la longitud de un vector, ni el ángulo entre los vectores, resultando imposible el desarrollo de la rica teoría geométrica, que conoce bien el lector para $n = 2$ y $n = 3$. Sin embargo la situación tiene salida del modo siguiente.

Por el curso de geometría analítica se sabe que en el plano y en el espacio de tres dimensiones se puede introducir el concepto de producto escalar de vectores. Este se define mediante la longitud de los vectores y el ángulo formado por ellos. No obstante, resulta que la longitud del vector y el ángulo formado por los vectores se pueden expresar a su vez mediante los productos escalares. Por esto, definiremos axiomáticamente el producto escalar en cualquier espacio lineal de n dimensiones mediante algunas propiedades bien conocidas del producto escalar de vectores en el plano o en el espacio de tres dimensiones. Además, teniendo en cuenta los objetivos inmediatos, debido a los cuales fue introducido este apartado en el curso de álgebra superior, aquí no se dará la definición de longitud de un vector y de ángulo entre los vectores. Al lector que le interese la construcción de la geometría en el espacio de n dimensiones le recomendamos que consulte literatura más especializada; en primer lugar, la del álgebra lineal.

En este capítulo, a excepción del final del presente párrafo, se examinan siempre los espacios lineales **reales.**

Diremos que en el espacio lineal real V_n de n dimensiones está definido el *producto escalar*, si a cada par de vectores a, b se ha puesto en correspondencia un número real, designado por la notación (a, b) y denominado *producto escalar* de los vectores a y b, cumpliéndose las condiciones siguientes (aquí, a, b, c son vectores arbitrarios del espacio V_n, α es un número real cualquiera):

I. $$(a, b) = (b, a).$$

II. $$(a+b, c)=(a, c)+(b, c).$$

III. $$(\alpha a, b)=\alpha(a, b).$$

IV. Si $a \neq 0$, el cuadrado escalar del vector a es estrictamente positivo,

$$(a, a)>0.$$

De III, para $\alpha=0$ se deduce la igualdad

$$(0, b)=0, \tag{1}$$

o sea, *el producto escalar del vector nulo por cualquier vector b es igual a cero*; en particular, es igual a cero el cuadrado escalar del vector nulo.

De II y III, se obtiene inmediatamente la siguiente **fórmula para el producto escalar de las combinaciones lineales de dos sistemas de vectores:**

$$\left(\sum_{i=1}^{k} \alpha_i a_i, \sum_{j=1}^{l} \beta_j b_j\right)=\sum_{i=1}^{k} \alpha_i \beta_j (a_i, b_j). \tag{2}$$

Si en el espacio lineal de n dimensiones está definido el producto escalar, éste se llama *espacio euclídeo* de n dimensiones.

Para cualquier n, se puede definir el producto escalar en el espacio lineal V_n de n dimensiones, o sea, este espacio se puede convertir en euclídeo.

En efecto, tomemos en el espacio V_n cualquier base $e_1, e_2, \ldots, e_n$. Si

$$a=\sum_{i=1}^{n} \alpha_i e_i, \quad b=\sum_{i=1}^{n} \beta_i e_i,$$

suponemos,

$$(a, b)=\sum_{i=1}^{n} \alpha_i \beta_i. \tag{3}$$

Fácilmente se comprueba que se cumplen las condiciones I-IV, o sea, que la igualdad (1) determina el producto escalar en el espacio V_n.

Vemos, pues, que generalmente, en el espacio lineal de n dimensiones se puede definir el producto escalar de muchos modos; naturalmente, la definición (3) depende de la elección de la base. Sin embargo, no sabemos por ahora si el producto escalar se puede introducir de algún modo que de principio sea diferente. Nuestro próximo objetivo consiste en examinar todos los modos posibles de convertir el espacio lineal de n dimensiones en espacio euclídeo y en establecer que, en cierto sentido, para cualquier n existe un solo espacio euclídeo de n dimensiones.

Sea dado un espacio euclídeo arbitrario E_n de n dimensiones, o sea, que en el espacio lineal de n dimensiones está definido arbitrariamente el producto escalar. Se dice que los vectores a y b son *ortogonales*, si su producto escalar es igual a cero,

$$(a, b) = 0.$$

De (1) se deduce que el vector nulo es ortogonal a cualquier vector; sin embargo, pueden existir también vectores ortogonales no nulos.

Un sistema de vectores se denomina *sistema ortogonal*, si todos los vectores de este sistema son ortogonales entre sí dos a dos.

Todo sistema ortogonal de vectores no nulos es linealmente independiente.

En efecto, sea dado en E_n un sistema de vectores $a_1, a_2, \ldots, a_k$, donde $a_i \neq 0$, $i = 1, 2, \ldots, k$, y

$$(a_i, a_j) = 0 \text{ para } i \neq j. \tag{4}$$

Si

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k = 0,$$

multiplicando escalarmente ambos miembros de esta igualdad por el vector a_i, $1 \leqslant i \leqslant k$, en virtud de (1), (2) y (4), resulta:

$$0 = (0, a_i) = (\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k, a_i) =$$
$$= \alpha_1 (a_1, a_i) + \alpha_2 (a_2, a_i) + \ldots + \alpha_k (a_k, a_i) = \alpha_i (a_i, a_i).$$

De aquí, como $(a_i, a_i) > 0$ según IV, se tiene $\alpha_i = 0$, $i = 1, 2, \ldots$ $\ldots, k$, como se quería demostrar.

Ahora se va a describir el **proceso de ortogonalización,** o sea, un método para pasar de cualquier sistema de k vectores

$$a_1, a_2, \ldots, a_k \tag{5}$$

linealmente independiente, del espacio euclídeo E_n, a un sistema ortogonal, compuesto también de k vectores no nulos; estos vectores se indicarán mediante $b_1, b_2, \ldots, b_k$.

Hagamos $b_1 = a_1$, de modo que **el primer vector del sistema** (5) **quedará incluido en el sistema ortogonal que se construye.** Hagamos luego

$$b_2 = \alpha_1 b_1 + a_2.$$

Como $b_1 = a_1$ y los vectores a_1 y a_2 son linealmente independientes, el vector b_2 será diferente de cero para cualquier número α_1. Elijamos este número de modo que el vector b_2 sea ortogonal al vector b_1:

$$0 = (b_1, b_2) = (b_1, \alpha_1 b_1 + a_2) = \alpha_1 (b_1, b_1) + (b_1, a_2),$$

de donde, en virtud de IV,

$$\alpha_1 = -\frac{(b_1, a_2)}{(b_1, b_1)}.$$

Supongamos que ya está construido el sistema ortogonal de vectores no nulos $b_1, b_2, \ldots, b_l$; supongamos, además, que para *cualquier* i, $1 \leqslant i \leqslant l$, *el vector* b_i *es combinación lineal de los vectores* $a_1, a_2, \ldots, a_i$. Entonces, esto mismo se cumplirá también para el vector b_{l+1}, si éste se elige de la forma siguiente:

$$b_{l+1} = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_l b_l + a_{l+1}.$$

En este caso, el vector b_{l+1} será diferente de cero, puesto que el sistema (5) es linealmente independiente y el vector a_{l+1} no está incluido entre los vectores $b_1, b_2, \ldots, b_l$. Los coeficientes α_i, $i = 1, 2, \ldots$ $\ldots, l$ se eligen de modo que el vector b_{l+1} sea ortogonal a todos los vectores b_i, $i = 1, 2, \ldots, l$:

$$0 = (b_i, b_{l+1}) = (b_i, \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_l b_l + a_{l+1}) =$$
$$= \alpha_1 (b_i, b_1) + \alpha_2 (b_i, b_2) + \ldots + \alpha_l (b_i, b_l) + (b_i, a_{l+1});$$

de aquí, como los vectores $b_1, b_2, \ldots, b_l$ son ortogonales entre sí, resulta

$$\alpha_i (b_i, b_i) + (b_i, a_{l+1}) = 0,$$

o sea,

$$\alpha_i = -\frac{(b_i, a_{l+1})}{(b_i, b_i)}, \quad i = 1, 2, \ldots, l.$$

Continuando este proceso se construye el sistema ortogonal buscado $b_1, b_2, \ldots, b_k$.

Aplicando este proceso de ortogonalización a cualquier base del espacio E_n, se obtiene un sistema ortogonal de n vectores no nulos, es decir una *base ortogonal*, pues, por lo demostrado, este sistema es linealmente independiente. Recordando ahora la observación hecha con relación al primer paso del proceso de ortogonalización y teniendo en cuenta también que cualquier vector no nulo se puede incluir en una base del espacio, se puede enunciar incluso la siguiente afirmación:

Todo espacio euclídeo posee bases ortogonales; cualquier vector no nulo de este espacio forma parte de alguna base ortogonal.

En adelante, desempeñará un papel importante una forma especial de base ortogonal; las bases de esta forma corresponden a los sistemas cartesianos rectangulares de coordenadas empleados en la geometría analítica.

El vector b se llamará *normal*, si su cuadrado escalar es igual a la unidad,

$$(b, b) = 1.$$

Si $a \neq 0$, de donde $(a, a) > 0$, el paso al vector

$$b = \frac{1}{\sqrt{(a, a)}}\, a$$

se denominará *normalización* del vector a. El vector b es normal, puesto que

$$(b, b) = \left(\frac{1}{\sqrt{(a, a)}}a, \frac{1}{\sqrt{(a, a)}}a\right) = \left(\frac{1}{\sqrt{(a, a)}}\right)^2 (a, a) = 1.$$

Una base $e_1, e_2, \ldots, e_n$ del espacio euclídeo E_n se llama *ortonormal*, si ésta es ortogonal y todos sus vectores son normales, es decir, si

$$\begin{aligned} (e_i, e_j) &= 0 \text{ para } i \neq j, \\ (e_i, e_i) &= 1, \qquad i = 1, 2, \ldots, n. \end{aligned} \tag{6}$$

Todo espacio euclídeo posee bases ortonormales.

Para la demostración es suficiente tomar cualquier base ortogonal y normalizar todos sus vectores. Con esto, la base se mantiene ortogonal, puesto que, para cualesquiera α y β, de $(a, b) = 0$, se deduce que

$$(\alpha a, \beta b) = \alpha\beta (a, b) = 0.$$

La base $e_1, e_2, \ldots, e_n$ del espacio euclídeo E_n es ortonormal si, y sólo si, el producto escalar de dos vectores cualesquiera del espacio es igual a la suma de los productos de las coordenadas correspondientes de estos vectores en la base indicada, o sea, si de

$$a = \sum_{i=1}^{n} \alpha_i e_i, \quad b = \sum_{j=1}^{n} \beta_j e_j \tag{7}$$

se deduce que

$$(a, b) = \sum_{i=1}^{n} \alpha_i \beta_i. \tag{8}$$

En efecto, si para nuestra base se verifican las igualdades (6), se tiene

$$(a, b) = \left(\sum_{i=1}^{n} \alpha_i e_i, \sum_{j=1}^{n} \beta_j e_j\right) = \sum_{i, j=1}^{n} \alpha_i \beta_j (e_i, e_j) = \sum_{i=1}^{n} \alpha_i \beta_i.$$

Recíprocamente, si nuestra base es tal, que para cualesquiera vectores a y b expresados en esta base en la forma (7) se cumple la igualdad (8), entonces, tomando por a y b dos vectores cualesquiera de esta base e_i y e_j, iguales o diferentes, las igualdades (6) se obtendrán de (8).

Confrontando este resultado obtenido con la demostración anterior de la existencia de espacios euclídeos de n dimensiones para cualquier n, se puede enunciar la siguiente proposición: *si en el espacio lineal de n dimensiones V_n se ha elegido una base arbitraria, en V_n se puede definir el producto escalar de modo que en el espacio euclídeo obtenido la base elegida sea una de las bases ortonormales.*

Isomorfismo de los espacios euclídeos. Se dice que los espacios euclídeos E y E' son *isomorfos*, si entre los vectores de los mismos se puede establecer una correspondencia biunívoca tal, que se cumplan las condiciones siguientes:

1) esta correspondencia es una correspondencia de isomorfismo entre E y E', considerados éstos como espacios lineales (véase el § 29);

2) *en esta correspondencia se conserva el producto escalar; en* otras palabras, si las imágenes de los vectores a y b de E son los vectores a' y b' de E', respectivamente, entonces

$$(a, b) = (a', b'). \tag{9}$$

De la condición 1) se deduce inmediatamente que *los espacios euclídeos isomorfos tienen una misma dimensión.* Demostremos la afirmación recíproca:

Dos espacios euclídeos cualesquiera E y E' que tengan una dimensión n, son isomorfos entre sí.

En efecto, elijamos en los espacios E y E' las bases **ortonormales**

$$e_1, e_2, \ldots, e_n \tag{10}$$

y, respectivamente,

$$e'_1, e'_2, \ldots, e'_n. \tag{11}$$

Poniendo en correspondencia a cada vector

$$a = \sum_{i=1}^{n} \alpha_i e_i$$

de E el vector

$$a' = \sum_{i=1}^{n} \alpha_i e'_i$$

de E', que tiene en la base (11) las mismas coordenadas que tiene el vector a en la base (10), se obtiene, evidentemente, una correspondencia de isomorfismo entre los espacios **lineales** E y E'. Demostremos que también se cumple la igualdad (9): si

$$b = \sum_{i=1}^{n} \beta_i e_i, \quad b' = \sum_{i=1}^{n} \beta_i e'_i,$$

entonces, en virtud de (8) (téngase en cuenta que las bases (10) y (11) son ortonormales),

$$(a, b) = \sum_{i=1}^{n} \alpha_i \beta_i = (a', b').$$

Es natural que los espacios euclídeos isomorfos no se deben considerar diferentes. Por esto, para cualquier n, existe solamente un espacio euclídeo de n dimensiones en el mismo sentido en que para cualquier n existe solamente un espacio lineal real de n dimensiones.

Para el caso de espacios lineales **complejos**, los conceptos y resultados del presente párrafo se generalizan del modo siguiente: un espacio lineal complejo se llama *espacio unitario*, si en él está definido el producto escalar, donde (a, b) es, por lo general, un número complejo. En este caso, tienen que cumplirse los axiomas II—IV (en el enunciado del último axioma se debe subrayar que el cuadrado escalar de todo vector no nulo es real y estrictamente positivo); el axioma I tiene que sustituirse por el axioma

I′ $$(a, b) = \overline{(b, a)},$$

donde la raya señala, como es usual, el paso al número complejo conjugado.

Por consiguiente, el producto escalar ya no es conmutativo. A pesar de todo, se verifica una igualdad simétrica al axioma II,

II′ $$(a, b+c) = (a, b) + (a, c),$$

ya que

$$(a, b+c) = \overline{(b+c, a)} = \overline{(b, a)+(c, a)} = \overline{(b, a)} + \overline{(c, a)} = (a, b) + (a, c).$$

Por otra parte,

III′ $$(a, \alpha b) = \bar{\alpha}(a, b),$$

puesto que

$$(a, \alpha b) = \overline{(\alpha b, a)} = \overline{\alpha (b, a)} = \bar{\alpha}\, \overline{(b, a)} = \bar{\alpha}(a, b).$$

Los conceptos de sistema ortogonal y ortonormal de vectores se generalizan sin alteración alguna al caso de espacios unitarios. Igual que antes, se demuestra la existencia de bases ortonormales en cualquier espacio unitario de dimensión finita. Sin embargo, si en este caso $e_1, e_2, \ldots, e_n$ es una base ortonormal y los vectores a, b tienen en esta base la expresión (7), se tiene

$$(a, b) = \sum_{i=1}^{n} \alpha_i \bar{\beta}_i.$$

Los resultados de los párrafos posteriores del presente capítulo también se podrían generalizar para el caso de espacios unitarios. Aquí no lo haremos y proponemos al lector que le interese que consulte libros especializados en álgebra lineal.

§ 35. Matrices ortogonales, transformaciones ortogonales

Sea dada una transformación lineal real de n indeterminadas

$$x_i = \sum_{k=1}^{n} q_{ik} y_k, \quad i = 1, 2, \ldots, n; \tag{1}$$

la matriz de esta transformación se denotará por Q. Esta transformación lleva la suma de cuadrados de las indeterminadas $x_1, x_2, \ldots, x_n$, o sea, la forma cuadrática $x_1^2 + x_2^2 + \ldots + x_n^2$, que es la forma normal de las formas cuadráticas definidas positivas (véase el § 28), a cierta forma en las indeterminadas $y_1, y_2, \ldots, y_n$. Eventualmente, esta nueva forma cuadrática también puede resultar ser la suma de los cuadrados de las indeterminadas $y_1, y_2, \ldots, y_n$, es decir, puede ocurrir que se verifique la igualdad

$$x_1^2+x_2^2+\ldots+x_n^2=y_1^2+y_2^2+\ldots+y_n^2, \tag{2}$$

lo cual se convierte en una identidad después de sustituir las indeterminadas $x_1, x_2, \ldots, x_n$ por sus expresiones (1). La transformación lineal de las indeterminadas (1) que posee esta propiedad, o como suele decirse, que mantiene invariante la suma de los cuadrados de las indeterminadas, se llama *transformación ortogonal de las indeterminadas*, y su matriz Q, *matriz ortogonal*.

Existen muchas otras definiciones de transformación ortogonal y de matriz ortogonal, equivalentes a la expuesta anteriormente. Indiquemos algunas de ellas que emplearemos después.

Ya conocemos, por el § 26, la ley según la cual se transforma la matriz de una forma cuadrática al realizar una transformación lineal de las indeterminadas. Aplicándola a nuestro caso y teniendo en cuenta que la matriz de la forma cuadrática, que es la suma *de los cuadrados de todas las indeterminadas, es la matriz unidad* E, resulta que la igualdad (2) es equivalente a la igualdad matricial

$$Q'EQ=E,$$

o sea,

$$Q'Q=E. \tag{3}$$

De aquí que

$$Q'=Q^{-1}, \tag{4}$$

por lo que también se cumple la igualdad

$$QQ'=E. \tag{5}$$

Por consiguiente, en virtud de (4), *la matriz ortogonal Q se puede definir como una matriz para la que la matriz transpuesta Q' es igual a la matriz inversa Q^{-1}*. Cada una de las igualdades (3) y (5) se puede tomar también por definición de matriz ortogonal.

Como las columnas de la matriz Q' son filas de la matriz Q, de (5) se deduce la proposición siguiente: *la matriz cuadrada Q es ortogonal cuando, y sólo cuando, la suma de los cuadrados de todos los elementos de cualquiera de sus filas es igual a la unidad y la suma de los productos de los elementos correspondientes de dos filas cualesquiera diferentes es igual a cero*. De (3) se deduce la proposición análoga para las columnas de la matriz Q.

Como $|Q'|=|Q|$, pasando a determinantes en la igualdad (3), resulta la igualdad

$$|Q|^2=1.$$

De aquí se deduce que *el determinante de una matriz ortogonal es igual a ± 1*. Por lo tanto, *toda transformación ortogonal de las inde-*

terminadas es no degenerada. Naturalmente, no se puede afirmar lo recíproco; señalemos también que no cualquier matriz con el determinante igual a ± 1 es ortogonal.

La matriz inversa de una matriz ortogonal es también ortogonal. En efecto, pasando en (4) a las matrices traspuestas, resulta:

$$(Q^{-1}) = (Q')' = Q = (Q^{-1})^{-1}.$$

Por otra parte, *el producto de matrices ortogonales también es ortogonal.* En efecto, si las matrices Q y R son ortogonales, entones aplicando (4) y también la igualdad (6) del § 26 y la igualdad análoga que se verifica para la matriz inversa, resulta:

$$(QR)' = R'Q' = R^{-1}Q^{-1} = (QR)^{-1}.$$

En el § 37 se empleará la proposición siguiente:

La matriz de cambio para pasar de una base ortonormal del espacio euclídeo a otra base ortonormal cualquiera es ortogonal.

En efecto, supongamos que en el espacio E_n se han dado dos bases ortonormales $e_1, e_2, \ldots, e_n$ y $e'_1, e'_2, \ldots, e'_n$ con la matriz de cambio $Q = (q_{ij})$,

$$e' = Qe.$$

Como la base e es ortonormal, el producto escalar de dos vectores cualesquiera y, en particular, de dos vectores cualesquiera de la base e', es igual a la suma de los productos de las coordenadas correspondientes de estos vectores en la base e. Sin embargo, como la base e' también es ortonormal, el cuadrado escalar de cada vector de e' es igual a la unidad, y el producto escalar de dos vectores diversos cualesquiera de e' es igual a cero. De aquí, para las filas de las coordenadas de los vectores de la base e' en la base e, o sea, para las filas de la matriz Q, resultan las afirmaciones que son características para una matriz ortogonal, como se dedujo antes de la igualdad (5).

Transformaciones ortogonales del espacio euclídeo. Ahora se estudiará un tipo especial e interesante de transformaciones lineales de los espacios euclídeos, a pesar de que estas transformaciones no se emplearán a continuación.

Una transformación lineal φ del espacio euclídeo E_n se llama *transformación ortogonal* de éste, si mantiene invariable el cuadrado escalar de cada vector, es decir, si para cualquier vector a

$$(a\varphi,\ a\varphi) = (a,\ a). \tag{6}$$

Ahora deduciremos la siguiente proposición más general que la anterior y que, naturalmente, también se puede tomar por definición de transformación ortogonal.

Toda transformación ortogonal φ del espacio euclídeo mantiene invariable el producto escalar de dos vectores cualesquiera a y b,

$$(a\varphi,\ b\varphi) = (a,\ b). \tag{7}$$

En efecto, en virtud de (6),

$$((a+b)\varphi,\ (a+b)\varphi) = (a+b,\ a+b).$$

Pero

$$((a+b)\varphi,\ (a+b)\varphi) = (a\varphi + b\varphi,\ a\varphi + b\varphi) =$$
$$= (a\varphi,\ a\varphi) + (a\varphi,\ b\varphi) + (b\varphi,\ a\varphi) + (b\varphi,\ b\varphi),$$
$$(a+b,\ a+b) = (a,\ a) + (a,\ b) + (b,\ a) + (b,\ b).$$

De aquí, aplicando (6) para a y para b, y teniendo en cuenta la propiedad conmutativa del producto escalar, resulta

$$2(a\varphi,\ b\varphi) = 2(a,\ b),$$

de donde, también se verifica (7).

En una transformación ortogonal del espacio euclídeo, las imágenes de todos los vectores de cualquier base ortonormal forman ellas mismas una base ortonormal. Recíprocamente, si una transformación lineal del espacio euclídeo transforma por lo menos una base ortonormal en otra base ortonormal, esta transformación es ortogonal.

En efecto, sea φ una transformación ortogonal del espacio sea E_n, y sea $e_1, e_2, \ldots, e_n$ una base ortonormal arbitraria de este espacio. En virtud de (7), de las igualdades

$$(e_i,\ e_i) = 1,\quad i = 1,\ 2,\ \ldots,\ n,$$
$$(e_i,\ e_j) = 0 \quad \text{para } i \neq j$$

se deducen las igualdades

$$(e_i\varphi,\ e_i\varphi) = 1,\quad i = 1,\ 2,\ \ldots,\ n,$$
$$(e_i\varphi,\ e_j\varphi) = 0 \quad \text{para } i \neq j,$$

o sea, el sistema de vectores $e_1\varphi, e_2\varphi, \ldots, e_n\varphi$ resulta ortogonal y normal, por lo cual, éste es una base ortonormal del espacio E_n.

Recíprocamente, supongamos que la transformación lineal φ del espacio E_n transforma la base ortonormal $e_1, e_2, \ldots, e_n$ de nuevo en una base ortonormal, es decir, que el sistema de vectores $e_1\varphi, e_2\varphi, \ldots, e_n\varphi$ es una base ortonormal del espacio E_n. Si

$$a = \sum_{i=1}^{n} \alpha_i e_i$$

es un vector arbitrario del espacio E_n, entonces

$$a\varphi = \sum_{i=1}^{n} \alpha_i (e_i\varphi),$$

o sea, el vector $a\varphi$ tiene en la base $e\varphi$ las mismas coordenadas que tiene el vector a en la base e. Sin embargo, ambas bases son ortonormales, siendo, por consiguiente, el cuadrado escalar de cualquier vector igual a la suma de los cuadrados de sus coordenadas en cualquiera de estas bases. Por lo tanto,

$$(a, a) = (a\varphi, a\varphi) = \sum_{i=1}^{n} \alpha_i^2,$$

o sea, se cumple verdaderamente la igualdad (6).

Toda transformación ortogonal del espacio euclídeo se determina en cualquier base ortonormal por una matriz ortogonal. Recíprocamente, si una transformación lineal del espacio euclídeo se determina por una matriz ortogonal, aunque sólo sea en una base ortonormal, esta transformación es ortogonal.

En efecto, si la transformación φ es ortogonal y la base $e_1, e_2, \ldots, e_n$ es ortonormal, el sistema de vectores $e_1\varphi, e_2\varphi, \ldots, e_n\varphi$ será una base ortonormal. Por consiguiente, la matriz A de la transformación φ en la base e,

$$e\varphi = Ae, \tag{8}$$

será la matriz de cambio de la base ortonormal e por la base ortonormal $e\varphi$, y, por lo demostrado anteriormente, es ortogonal.

Recíprocamente, supongamos que la transformación lineal φ se determina en la base ortonormal $e_1, e_2, \ldots, e_n$ por la matriz ortogonal A; por consiguiente, se cumple la igualdad (8). Como la base e es ortonormal, el producto escalar de cualesquiera vectores y, en particular, de cualesquiera vectores del sistema $e_1\varphi, e_2\varphi, \ldots, e_n\varphi$, es igual a la suma de los productos de las coordenadas correspondientes de estos vectores en la base e. De donde, como la matriz A es ortogonal, se tiene

$$(e_i\varphi, e_i\varphi) = 1, \quad i = 1, 2, \ldots, n$$
$$(e_i\varphi, e_j\varphi) = 0 \quad \text{para } i \neq j,$$

o sea, resulta que el mismo sistema e es una base ortonormal del espacio E_n. De aquí se deduce que la transformación φ es ortogonal.

Por la geometría analítica sabemos, que entre todas las transformaciones afines del plano que dejan en su sitio el origen de coordenadas, las rotaciones (unidas, posiblemente, con simetrías) son las únicas que mantienen invariante el producto escalar. Por lo tanto, las transformaciones ortogonales del espacio euclídeo de n dimensiones se pueden considerar como «rotaciones» de este espacio.

Evidentemente, entre las transformaciones ortogonales del espacio euclídeo está también la transformación idéntica. Por otra parte, la relación que hemos establecido entre las transformaciones ortogonales y las matrices ortogonales, y también la relación expuesta en el § 31 entre las operaciones con las transformaciones lineales y con las matrices, permiten deducir de las propiedades conocidas de las matrices ortogonales las siguientes propiedades de las transformaciones ortogonales del espacio euclídeo, que también se comprueban directamente con facilidad:

Toda transformación ortogonal es no degenerada y su transformación inversa también es ortogonal.

El producto de cualesquiera transformaciones ortogonales es ortogonal.

§ 36. Transformaciones simétricas

Una transformación lineal del espacio euclídeo de n dimensiones se llama *simétrica* (o bien, *autoconjugada*) si para cualesquiera vectores a, b de este espacio se verifica la igualdad

$$(a\varphi,\ b) = (a,\ b\varphi) \tag{1}$$

o sea, en el producto escalar el símbolo de la transformación simétrica se puede trasladar de un factor a otro.

Evidentemente, la transformación idéntica ε y la transformación nula ω son ejemplos de transformaciones simétricas. Un ejemplo más general es la transformación lineal, según la cual cada vector se multiplica por un número fijado α,

$$a\varphi = \alpha a.$$

En efecto, en este caso

$$(a\varphi,\ b) = (\alpha a,\ b) = \alpha (a,\ b) = (a,\ \alpha b) = (a,\ b\varphi).$$

Las transformaciones simétricas desempeñan un papel muy importante y es necesario estudiarlas detalladamente.

Toda transformación simétrica del espacio euclídeo se determina en cualquier base ortonormal por una matriz simétrica. Recíprocamente, si una transformación lineal del espacio euclídeo se determina por una matriz simétrica, aunque sólo sea en una base ortonormal, la transformación es simétrica.

En efecto, supongamos que la transformación simétrica φ se determina por la matriz $A = (\alpha_{ij})$ en la base ortonormal $e_1,\ e_2,\ \ldots$ $\ldots,\ e_n$. Teniendo en cuenta que en una base ortonormal, el producto escalar de dos vectores es igual a la suma de los productos de las coordenadas correspondientes de estos vectores, se obtiene:

$$(e_i\varphi,\ e_j) = \Big(\sum_{k=1}^{n} \alpha_{ik} e_k,\ e_j\Big) = \alpha_{ij},$$

$$(e_i,\ e_j\varphi) = \Big(e_i,\ \sum_{k=1}^{n} \alpha_{jk} e_k\Big) = \alpha_{ji},$$

o sea, en virtud de (1),

$$\alpha_{ij} = \alpha_{ji}$$

para todos los valores de i y j. De aquí, la matriz A es simétrica.

Recíprocamente, supongamos que la transformación lineal φ se determina por una matriz simétrica $A = (\alpha_{ij})$ en la base ortonormal $e_1, e_2, \ldots, e_n$,

$$\alpha_{ij} = \alpha_{ji} \text{ para todos los valores de } i \text{ y } j. \tag{2}$$

Si

$$b = \sum_{i=1}^{n} \beta_i e_i, \quad c = \sum_{j=1}^{n} \gamma_j e_j$$

son unos vectores arbitrarios del espacio, entonces

$$b\varphi = \sum_{i=1}^{n} \beta_i (e_i\varphi) = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \beta_i \alpha_{ij} \right) e_j,$$

$$c\varphi = \sum_{j=1}^{n} \gamma_j (e_j\varphi) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} \gamma_j \alpha_{ji} \right) e_i.$$

Teniendo en cuenta que la base e es ortonormal, resulta

$$(b\varphi, c) = \sum_{j, i=1}^{n} \beta_i \alpha_{ij} \gamma_j,$$

$$(b, c\varphi) = \sum_{i, j=1}^{n} \beta_i \gamma_j \alpha_{ji}.$$

En virtud de (2), los segundos miembros de las últimas igualdades coinciden, así que

$$(b\varphi, c) = (b, c\varphi),$$

que es lo que se quería demostrar.

Del resultado obtenido se deduce la siguiente propiedad de las transformaciones simétricas, que también se comprueba con facilidad directamente:

La suma de transformaciones simétricas y también el producto de una transformación simétrica por un número, son transformaciones simétricas.

Demostremos ahora el siguiente importante teorema:

Todas las raíces características de una transformación simétrica son reales.

Como las raíces características de cualquier transformación lineal coinciden con las raíces características de la matriz de esta transformación en cualquier base y la transformación simétrica se determina en bases ortonormales por matrices simétricas, es suficiente demostrar la proposición siguiente:

Todas las raíces características de una matriz simétrica son reales.

En efecto, sea λ_0 una raíz característica (que puede ser compleja) de la matriz simétrica $A = (\alpha_{ij})$,

$$|A-\lambda_0 E|=0.$$

Entonces el sistema de ecuaciones lineales homogéneas con coeficientes complejos

$$\sum_{j=1}^{n} \alpha_{ij}x_j=\lambda_0 x_i, \quad i=1,\ 2,\ \ldots,\ n,$$

tiene un determinante igual a cero, o sea, posee solución **no nula** $\beta_1,\ \beta_2,\ \ldots,\ \beta_n$, *que por lo general, es compleja*; por lo tanto,

$$\sum_{i=1}^{n} \alpha_{ij}\beta_j=\lambda_0\beta_i,\ i=1,\ 2,\ \ldots,\ n. \tag{3}$$

Multiplicando ambos miembros de cada i-ésima igualdad (3) por el número $\overline{\beta}_i$, conjugado con el número β_i, y sumando por separado los primeros y los segundos miembros de todas las igualdades obtenidas, se llega a la igualdad

$$\sum_{i,\ j=1}^{n} a_{ij}\beta_j\overline{\beta}_i=\lambda_0 \sum_{i=1}^{n} \beta_i\overline{\beta}_i. \tag{4}$$

El coeficiente de λ_0 en la igualdad (4) es un número real, diferente de cero, puesto que es la suma de números reales no negativos, uno de los cuales por lo menos es estrictamente positivo. Para demostrar *que el número λ_0 es real*, hay que demostrar que es real el primer miembro de la igualdad (4), para lo cual es suficiente demostrar que este número complejo coincide con su conjugado. Aquí, por primera vez se aplicará la simetría de la matriz (real) A:

$$\overline{\sum_{i,\ j=1}^{n} \alpha_{ij}\beta_j\overline{\beta}_i}=\sum_{i,\ j=1}^{n} \overline{\alpha_{ij}\beta_j\overline{\beta}_i}=\sum_{i,\ j=1}^{n} \alpha_{ij}\overline{\beta}_j\beta_i=$$
$$=\sum_{i,\ j=1}^{n} \alpha_{ji}\overline{\beta}_j\beta_i=\sum_{i,\ j=1}^{n} \alpha_{ij}\overline{\beta}_i\beta_j=\sum_{i,\ j=1}^{n} \alpha_{ij}\beta_j\overline{\beta}_i.$$

Obsérvese que la penúltima igualdad se ha obtenido mediante una permutación simple de las notaciones de los índices de la suma: en lugar de i se ha puesto j, y en lugar de j se ha puesto i. Por consiguiente, el teorema queda demostrado.

Una transformación lineal φ del espacio euclídeo E_n es simétrica cuando, y sólo cuando, en el espacio E_n existe una base ortonormal formada por vectores propios de esta transformación.

Una parte de esta proposición es casi evidente: si en E_n existe una base ortonormal $e_1,\ e_2,\ \ldots,\ e_n$ tal que

$$e_i\varphi=\lambda_i e_i,\ i=1,\ 2,\ \ldots,\ n,$$

entonces en la base e la transformación φ se determina por la matriz diagonal

$$\begin{pmatrix} \lambda_1 & & & & 0 \\ & \lambda_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ 0 & & & & \lambda_n \end{pmatrix}.$$

Pero, como toda matriz diagonal es simétrica resulta que la transformación φ se determina en la base ortonormal e por una matriz simétrica, es decir, ella misma es simétrica.

La proposición recíproca fundamental se demostrará por inducción sobre la dimensión n del espacio E_n. En efecto, para $n = 1$ cualquier transformación lineal φ del espacio E_1 lleva cualquier vector a otro que es proporcional al mismo. De esto se deduce que todo vector a no nulo es un vector propio para φ (por cierto, resulta también que toda transformación lineal del espacio E_1 es simétrica). Normalizando el vector a se obtiene la base ortonormal buscada del espacio E_1.

Supongamos que la tesis del teorema ya está demostrada para los espacios euclídeos de $(n - 1)$ dimensiones y que en el espacio E_n se ha dado una transformación simétrica φ. Del teorema demostrado anteriormente se deduce la existencia de una raíz característica real λ_0 para φ. Por consiguiente, para la transformación φ, este número es un valor propio. Si a es el vector propio de la transformación φ que corresponde a este valor propio, entonces cualquier vector no nulo que sea proporcional al vector a será para φ un vector propio correspondiente al mismo valor propio λ_0, puesto que

$$(\alpha a)\varphi = \alpha(a\varphi) = \alpha(\lambda_0 a) = \lambda_0(\alpha a).$$

En particular, normalizando el vector a, resulta un vector e_1 tal que

$$e_1\varphi = \lambda_0 e_1,$$
$$(e_1, e_1) = 1.$$

Como se demostró en el § 34, el vector no nulo e_1 se puede incluir en una base ortogonal

$$e_1, e_2', \ldots, e_n' \tag{5}$$

del espacio E_n. Los vectores cuyas primeras coordenadas en la base (5) son iguales a cero, o sea, los vectores de la forma $\alpha_2 e_2' + \ldots + \alpha_n e_n'$, forman, evidentemente, un subespacio lineal de $(n - 1)$ dimensiones del espacio E_n, que lo designaremos mediante L. Este será, incluso, un espacio euclídeo de $(n - 1)$ dimensiones, pues, estando definido el producto escalar para todos los vectores de E_n, lo estará particularmente para los vectores de L, poseyendo además todas las propiedades necesarias.

El subespacio L consta de todos los vectores del espacio E_n que son ortogonales al vector e_1. En efecto, si

$$a = \alpha_1 e_1 + \alpha_2' e_2' + \ldots + \alpha_n' e_n',$$

como la base (5) es ortogonal y el vector e_1, normal, resulta

$$(e_1, a) = \alpha_1 (e_1, e_1) + \alpha_2' (e_1, e_2') + \ldots + \alpha_n' (e_1, e_n') = \alpha_1,$$

o sea, $(e_1, a) = 0$ cuando, y sólo cuando, $\alpha_1 = 0$.

Si el vector a pertenece al subespacio L, es decir, si $(e_1, a) = 0$, el vector $a\varphi$ también pertenecerá a L. En efecto, como la transformación φ es simétrica, resulta

$$(e_1, a\varphi) = (e_1\varphi, a) = (\lambda_0 e_1, a) = \lambda_0 (e_1, \alpha) = \lambda_0 \cdot 0 = 0,$$

o sea, el vector $a\varphi$ es ortogonal a e_1, estando por esto contenido en L. Esta propiedad del subespacio L, llamada *invariabilidad* con respecto a la transformación φ, permite considerar a φ, **aplicándola solamente a los vectores de** L, como una transformación lineal de este espacio euclídeo de $(n - 1)$ dimensiones. Esta será, incluso, una transformación simétrica del espacio L, pues, la igualdad (1), cumpliéndose para cualesquiera vectores de E_n, se cumple particularmente, para los vectores situados en L.

Por la suposición de la inducción, en el espacio L existe una base ortonormal compuesta de vectores propios de la transformación φ; designémosla mediante $e_2, \ldots, e_n$. Todos estos vectores son ortogonales al vector e_1; por consiguiente, $e_1, e_2, \ldots, e_n$ será la base ortonormal buscada del espacio E_n, que consta de vectores propios de la transformación φ. El teorema queda demostrado.

§ 37. Reducción de una forma cuadrática a los ejes principales. Par de formas

Apliquemos el último teorema del párrafo precedente para la demostración del siguiente teorema matricial:

Para cualquier matriz simétrica A se puede hallar una matriz ortogonal Q que reduzca la matriz A a la forma diagonal, o sea, que la matriz $Q^{-1}AQ$, que es la transformada de la matriz A por la matriz Q, resulta diagonal.

Sea dada una matriz simétrica A de orden n. Si $e_1, e_2, \ldots, e_n$ es una base ortonormal del espacio euclídeo E_n de n dimensiones, la matriz A determina en esta base una transformación simétrica φ. Por lo demostrado, en E_n existe una base ortonormal $f_1, f_2, \ldots, f_n$, compuesta de vectores propios de la transformación φ; en esta base, φ

se determina por una matriz diagonal B (véase el § 33). Entonces, en virtud del § 31,

$$B = Q^{-1}AQ, \tag{1}$$

donde Q es la matriz de cambio de la base f a la base e,

$$e = Qf. \tag{2}$$

Esta matriz, como matriz de cambio de una base ortonormal a otra base ortonormal, es ortogonal (véase el § 35). El teorema queda demostrado.

Como para una matriz ortogonal Q la matriz inversa es la transpuesta, $Q^{-1} = Q'$, la igualdad (1) se puede escribir en la forma

$$B = Q'AQ;$$

no obstante, por el § 26 se sabe que precisamente así se transforma la matriz simétrica A de una forma cuadrática, sometida a una transformación lineal de las indeterminadas de matriz Q. Teniendo en cuenta que una transformación lineal de las indeterminadas de matriz ortogonal es una transformación ortogonal (véase el §35) y que la forma cuadrática reducida a la forma canónica tiene una matriz diagonal, basándonos en el teorema precedente obtenemos el siguiente **teorema de reducción de una forma cuadrática real a los ejes principales:**

Toda forma cuadrática real $f(x_1, x_2, \ldots, x_n)$ se puede reducir a la forma canónica mediante una transformación ortogonal de las indeterminadas.

A pesar de que puedan existir muchas transformaciones ortogonales diferentes de las indeterminadas que reduzcan la forma cuadrática dada a la forma canónica, ésta se determina en lo fundamental unívocamente:

Cualquiera que sea la transformación ortogonal que reduzca la forma cuadrática $f(x_1, x_2, \ldots, x_n)$ de matriz A a la forma canónica, los coeficientes de esta forma canónica son las raíces características de la matriz A, tomadas con sus órdenes de multiplicidad.

En efecto, supongamos que la forma f se ha reducido ya a la forma canónica

$$f(x_1, x_2, \ldots, x_n) = \mu_1 y_1^2 + \mu_2 y_2^2 + \ldots + \mu_n y_n^2,$$

mediante una transformación ortogonal.

Esta transformación ortogonal mantiene invariable la suma de los cuadrados de las indeterminadas, de donde, si λ es una nueva indeterminada, se tiene

$$f(x_1, x_2, \ldots, x_n) - \lambda \sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} \mu_i y_i^2 - \lambda \sum_{i=1}^{n} y_i^2.$$

Pasando a los determinantes de estas formas cuadráticas y teniendo en cuenta que después de realizar la transformación lineal el determinante de la forma cuadrática se multiplica por el cuadrado del *determinante de la transformación (véase el § 28), y que el cuadrado* del determinante de una transformación ortogonal es igual a la unidad (véase el § 35), llegamos a la igualdad

$$|A-\lambda E| = \begin{vmatrix} \mu_1-\lambda & 0 & \dots & 0 \\ 0 & \mu_2-\lambda & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \mu_n-\lambda \end{vmatrix} = \prod_{i=1}^{n} (\mu_i-\lambda),$$

de la que se deduce la tesis del teorema.

Este resultado se puede formular también de una forma matricial:

Cualquiera que sea la matriz ortogonal que reduzca la matriz simétrica A a la forma diagonal, en la diagonal principal de la matriz diagonal obtenida figurarán las raíces características de la matriz A, tomadas con sus órdenes de multiplicidad.

Averiguación práctica de la transformación ortogonal que reduce una forma cuadrática a los ejes principales. En algunos problemas no sólo es necesario conocer la forma canónica a que se reduce una forma cuadrática real mediante una transformación ortogonal, sino también la transformación ortogonal que realiza esta reducción. Sería difícil buscar esta transformación empleando la demostración del teorema de reducción a los ejes principales, y queremos mostrar otro camino. Para esto sólo hace falta aprender a hallar la matriz ortogonal Q que reduce la matriz simétrica dada A a la forma diagonal o, lo que es lo mismo, a hallar su matriz inversa Q^{-1}. En virtud de (2), ésta es la matriz de cambio de la base e a la base f, es decir, sus filas son filas de las coordenadas (en la base e) del sistema ortonormal compuesto por n vectores propios de la transformación simétrica φ, determinada por la matriz A en la base e. No queda más que hallar tal sistema de vectores propios.

Sea λ_0 cualquier raíz característica de la matriz A y supongamos que su orden de multiplicidad es igual a k_0. Por el § 33 se sabe que el conjunto de las filas de coordenadas de todos los vectores propios de la transformación φ, correspondientes al valor propio λ_0, coincide con el conjunto de las soluciones no nulas del sistema de ecuaciones lineales homogéneas

$$(A-\lambda_0 E)\,X=0; \tag{3}$$

como la matriz A es simétrica, se puede escribir A en lugar de A'. De los teoremas de existencia de una matriz ortogonal que reduzca la matriz simétrica A a la forma diagonal, demostrados anteriormente, y de la unicidad de esta forma diagonal, se deduce que para el sistema (3) se pueden hallar siempre k_0 soluciones linealmente independientes. Este sistema de soluciones se halla por los métodos conocidos en el § 12, ortogonalizando y normalizando después el sistema obtenido según el § 34.

Tomando por λ_0 cada una de las raíces características distintas de la matriz simétrica A y teniendo en cuenta que la suma de los órdenes de multiplicidad de estas raíces es igual a n, se obtiene un sistema de n vectores propios de la transformación φ, dados por sus coordenadas en la base e. Para demostrar que éste es el sistema ortonormal de los vectores propios buscados, no queda más que demostrar el siguiente **lema**:

Los vectores propios de una transformación simétrica φ que corresponden a valores propios distintos son ortogonales entre sí.

En efecto, supongamos que

$$b\varphi = \lambda_1 b, \quad c\varphi = \lambda_2 c,$$

siendo $\lambda_1 \neq \lambda_2$. Como

$$(b\varphi,\ c) = (\lambda_1 b,\ c) = \lambda_1 (b,\ c),$$
$$(b,\ c\varphi) = (b,\ \lambda_2 c) = \lambda_2 (b,\ c),$$

de

$$(b\varphi,\ c) = (b,\ c\varphi)$$

se deduce que

$$\lambda_1 (b,\ c) = \lambda_2 (b,\ c)$$

y, puesto que $\lambda_1 \neq \lambda_2$, resulta

$$(b,\ c) = 0,$$

que es lo que se quería demostrar.

Ejemplo. Reducir la forma cuadrática

$$f(x_1,\ x_2,\ x_3,\ x_4) = 2x_1x_2 + 2x_1x_3 - 2x_1x_4 - 2x_2x_3 + 2x_2x_4 + 2x_3x_4$$

a los ejes principales.

La matriz A de esta forma es

$$A = \begin{pmatrix} 0 & 1 & 1 & -1 \\ 1 & 0 & -1 & 1 \\ 1 & -1 & 0 & 1 \\ -1 & 1 & 1 & 0 \end{pmatrix}.$$

Hallemos su polinomio característico:

$$|A - \lambda E| = \begin{vmatrix} -\lambda & 1 & 1 & -1 \\ 1 & -\lambda & -1 & 1 \\ 1 & -1 & -\lambda & 1 \\ -1 & 1 & 1 & -\lambda \end{vmatrix} = (\lambda - 1)^3 (\lambda + 3).$$

Por lo tanto, la matriz A tiene la raíz característica 1 de orden tres y la raíz característica simple -3. Por consiguiente, ya se puede escribir la forma canónica a que se reduce la forma f mediante una transformación ortogonal:

$$f=y_1^2+y_2^2+y_3^2-3y_4^2.$$

Hallemos la transformación ortogonal que realiza esta reducción. El sistema de ecuaciones lineales homogéneas (3) para $\lambda_0=1$ toma la forma

$$\begin{cases} -x_1+x_2+x_3-x_4=0, \\ x_1-x_2-x_3+x_4=0, \\ x_1-x_2-x_3+x_4=0, \\ -x_1+x_2+x_3-x_4=0. \end{cases}$$

El rango de este sistema es igual a 1. Por lo tanto, para éste se pueden hallar tres soluciones linealmente independientes. Estas son, por ejemplo, los vectores

$$\begin{aligned} b_1&=(1,\ 1,\ 0,\ 0), \\ b_2&=(1,\ 0,\ 1,\ 0). \\ b_3&=(-1,\ 0,\ 0,\ 1). \end{aligned}$$

Ortogonalizando este sistema de vectores, se obtiene el sistema de vectores

$$\begin{aligned} c_1&=b_1=(1,\ 1,\ 0,\ 0), \\ c_2&=-\frac{1}{2}c_1+b_2=\left(\frac{1}{2},\ -\frac{1}{2},\ 1,\ 0\right), \\ c_3&=\frac{1}{2}\,c_1+\frac{1}{3}\,c_2+b_3=\left(-\frac{1}{3},\ \frac{1}{3},\ \frac{1}{3},\ 1\right). \end{aligned}$$

Por otra parte, el sistema de ecuaciones lineales homogéneas (3) para $\lambda_0=-3$, toma la forma

$$\begin{cases} 3x_1+x_2+x_3-x_4=0, \\ x_1+3x_2-x_3+x_4=0, \\ x_1-x_2+3x_3+x_4=0, \\ -x_1+x_2+x_3+3x_4=0. \end{cases}$$

El rango de este sistema es igual a 3. El vector

$$c_4=(1,\ -1,\ -1,\ 1).$$

es una solución no nula.

El sistema de vectores c_1, c_2, c_3, c_4 es ortogonal. Normalizando este sistema llegamos al sistema ortonormal de vectores

$$\begin{aligned} c_1'&=\left(\frac{1}{\sqrt{2}},\ \frac{1}{\sqrt{2}},\ 0,\ 0\right), \\ c_2'&=\left(\frac{1}{\sqrt{6}},\ -\frac{1}{\sqrt{6}},\ \sqrt{\frac{2}{3}},\ 0\right), \\ c_3'&=\left(-\frac{1}{2\sqrt{3}},\ \frac{1}{2\sqrt{3}},\ \frac{1}{2\sqrt{3}},\ \frac{\sqrt{3}}{2}\right), \\ c_4'&=\left(\frac{1}{2},\ -\frac{1}{2},\ -\frac{1}{2},\ \frac{1}{2}\right). \end{aligned}$$

Por lo tanto, la forma f se reduce a los ejes principales mediante la transformación ortogonal

$$y_1 = \frac{1}{\sqrt{2}} x_1 + \frac{1}{\sqrt{2}} x_2,$$

$$y_2 = \frac{1}{\sqrt{6}} x_1 - \frac{1}{\sqrt{6}} x_2 + \sqrt{\frac{2}{3}} x_3,$$

$$y_3 = -\frac{1}{2\sqrt{3}} x_1 + \frac{1}{2\sqrt{3}} x_2 + \frac{1}{2\sqrt{3}} x_3 + \frac{\sqrt{3}}{2} x_4,$$

$$y_4 = \frac{1}{2} x_1 - \frac{1}{2} x_2 - \frac{1}{2} x_3 + \frac{1}{2} x_4.$$

Es menester señalar que la elección del sistema de vectores propios, linealmente independientes, correspondientes a un valor propio múltiple, goza de mucha pluralidad; de aquí que existan muchas transformaciones ortogonales distintas que reducen la forma f a la forma conónica. Aquí sólo hemos hallado una de éstas.

Par de formas. Sea dado *un par de formas cuadráticas en n indeterminadas*, $f(x_1, x_2, \ldots, x_n)$ y $g(x_1, x_2, \ldots, x_n)$. ¿Existe alguna transformación lineal no degenerada de las indeterminadas $x_1, x_2, \ldots, x_n$ que reduzca simultáneamente ambas formas a la forma canónica?

En el caso general, la respuesta es negativa. Veamos, por ejemplo, el par de formas

$$f(x_1, x_2) = x_1^2, \quad g(x_1, x_2) = x_1x_2.$$

Supongamos que existe una transformación lineal no degenerada

$$\left.\begin{aligned} x_1 &= c_{11}y_1 + c_{12}y_2, \\ x_2 &= c_{21}y_1 + c_{22}y_2, \end{aligned}\right\} \tag{4}$$

que reduce ambas formas a la forma canónica. Para que la forma f pueda reducirse por la transformación (4) a la forma canónica, uno de los coeficientes c_{11}, c_{12} tiene que ser igual a cero, si no aparecería el término $2c_{11}c_{12}y_1y_2$. Cambiando la numeración de las indeterminadas y_1, y_2, si esto fuese necesario, se puede suponer que $c_{12} = 0$, de donde $c_{11} \neq 0$. Sin embargo, ahora resulta que

$$g(x_1, x_2) = c_{11}y_1(c_{21}y_1 + c_{22}y_2) = c_{11}c_{21}y_1^2 + c_{11}c_{22}y_1y_2.$$

Como también la forma g tiene que reducirse a la forma canónica, tiene que ser $c_{11}c_{22} = 0$, es decir, $c_{22} = 0$, lo cual, junto con $c_{12} = 0$, nos lleva a lo absurdo, pues la transformación lineal (4) no es degenerada.

La situación será diferente si se supone que al menos una de nuestras formas, por ejemplo, $g(x_1, x_2, \ldots, x_n)$ es **definida positiva** *. Subsiste el teorema siguiente:

Si f y g es un par de formas cuadráticas reales en n indeterminadas, siendo la segunda de ellas definida positiva, existe una transformación lineal no degenerada que reduce simultáneamente la forma g a la forma normal y la forma f a la forma canónica.

Para la demostración, realicemos primero una transformación lineal no degenerada de las indeterminadas $x_1, x_2, \ldots, x_n$,

$$X = TY,$$

que reduzca la forma definida positiva g a la forma normal,

$$g(x_1, x_2, \ldots, x_n) = y_1^2 + y_2^2 + \ldots + y_n^2.$$

En este caso, la forma f se reducirá a otra forma φ en las nuevas indeterminadas,

$$f(x_1, x_2, \ldots, x_n) = \varphi(y_1, y_2, \ldots, y_n).$$

Realicemos ahora una transformación **ortogonal** de las indeterminadas $y_1, y_2, \ldots, y_n$,

$$Y = QZ,$$

que lleve la forma φ a los ejes principales,

$$\varphi(y_1, y_2, \ldots, y_n) = \lambda_1 z_1^2 + \lambda_2 z_2^2 + \ldots + \lambda_n z_n^2.$$

Esta transformación (véase la definición en el § 35) lleva la suma de los cuadrados de las indeterminadas $y_1, y_2, \ldots, y_n$ a la suma de los cuadrados de las indeterminadas $z_1, z_2, \ldots, z_n$. Por lo tanto, resulta

$$f(x_1, x_2, \ldots, x_n) = \lambda_1 z_1^2 + \lambda_2 z_2^2 + \ldots + \lambda_n z_n^2,$$
$$g(x_1, x_2, \ldots, x_n) = z_1^2 + z_2^2 + \ldots + z_n^2,$$

o sea, la transformación lineal

$$X = (TQ)Z$$

es la buscada.

* Claro, esta condición no es necesaria; así, pues, las formas $x_1 + x_2^2 - x_3^2$ y $x_1^2 - x_2^2 - x_3^2$ ya tienen la forma canónica, a pesar de que entre ellas no hay definidas positivas.